



Yvonne
Hofstetter

Láthatatlan háború

avagy miképpen fenyegeti
a digitalizáció a világ
biztonságát és stabilitását

Corvina



Yvonne
Hofstetter

Láthatatlan háború

avagy miképpen fenyegeti
a digitalizáció a világ
biztonságát és stabilitását

Corvina

Yvonne
Hofstetter

Láthatatlan háború

avagy miképpen fenyegeti
a digitalizáció a világ
biztonságát és stabilitását

CORVINA

A fordítás az alábbi kiadás alapján készült:
Yvonne Hofstetter: *Der unsichtbare Krieg. Wie die Digitalisierung Sicherheit und Stabilität in der Welt bedroht.*
Droehmer Verlag, München, 2019

© Yvonne Hofstetter, 2019
Published by arrangement with Michael Gaeb Literary
Agency, Berlin

Hungarian translation © Kőrös László, 2020

Borítóterv: Székelyhidi Zsolt, a besthqwallpapers.com
képének felhasználásával

Kiadja 2020-ban a Corvina Kiadó Kft., az 1795-ben alapított Magyar Könyvkiadók és Könyvterjesztők Egyesülésének tagja.

ISBN 978 963 13 6698 3

Elektronikus verzió:
eKönyv Magyarország Kft.
www.ekonyv.hu

Készítette: *Ambrose Montanus*

[ELŐSZÓ]

A béke kellős közepén

Digital first. Aggályoskodás second.

(A német Freie Demokratische Partei 2017-es választási plakátja)

Feladó: Anonymous Hekker

Dátum: 2019. július 30.

Címzett: yvonnehofstetter@web.de

Helló, áldozat! Ismerem a jelszavadat: torino2011. Ez az utolsó figyelmeztetésem. Azért írok, mert trójait telepítettem egy pornográf weboldalra. Te pedig látogatsz az oldalra. Az én malware-em meg rögzítette a személyes adataidat. Ezután elmentette a címlistádat és bekapcsolta a webkamerádat. Illetlenül viselkedtél, én pedig közben felvételt készítettem rólad. Csak akkor törölöm az adataidat és a mocskos videót, ha fizetsz 500 amerikai dollár értékű bitcoin. A bitcoin-pénztárcám címe: 135qVXXBZ-b3v2tQcLJRA8UAndiUYBnbh3J (Esetleg keress

rá: „Hogyan tudsz bitcoint venni?”) Huszon-
négy órát adok attól a pillanattól számít-
va, hogy elolvastad az értesítésemet. És
rögtön megtudom, ha elolvastad. Riaszthatod
a rendőrséget, de nem fognak segíteni. Ha
megpróbálsz becsapni, rögtön észreveszem!
Képzeld csak el, milyen kínos helyzetbe ke-
rülsz: tönkretéhetem az életedet!

* * *

Nem, soha nem látogattam el semmilyen pornóoldalra, és nincs
semmi látni- vagy hallanivaló nálam, ha egy hekker be találja
kapcsolni a laptopom vagy tabletem kameráját vagy mikrofon-
ját – merthogy jó néhány éve leragasztottam az elektronikus
eszközeim szenzorait. Így hát ez az e-mailes fenyegetés is csak
blöff. Ha Önök netán hasonló zsaroló e-maileket kapnának, ne
fizessenek. Ha pedig a fenyegető üzenetet egy további, csatolt
fájlt tartalmazó e-mail követné, eszükbe ne jusson megnyitni a
csatolmányt! Kártevő programot telepíthet a számítógépre.

Ennek a könyvnek az írása alatt számítógépes bűnözők egy-
szer megzsaroltak, egyszer megloptak, egyszer pedig meghek-
kelték a gépem. Saját számítástechnikai eszközeim biztonságá-
ról mindedig magam is képes voltam gondoskodni, de azoknak
az információknak a védelme, amelyeket át kellett engednem
más cégeknek, már nem az én gondosságomon múlik. Így példá-
ul a Dropboxnál, ahol az adattárolót támadás érte, és ellopták a

felhasználók e-mail-adatait. Vagy a Marriott szállodaláncnál, ahonnan 500 millió szállodavendég címét tulajdonították el, emellett sok hitelkártya-adatot is. Én is ügyfele vagyok a Marriottnak. A számlatulajdonosnak az adatlopás csak akkor nem okoz közvetlen pénzügyi veszteséget, ha a bank gyanút fog: „Az *Air Nigeriától* gyanús tranzakció-kérelmet kaptunk, ezért zároltuk a hitelkártyáját.” Ennek ellenére tetemes az online csalások által okozott nemzetgazdasági kár, ugyanis teljesen improdukív munkaráfordítást tesz szükségessé.

Amikor hekkertámadásokra derül fény, az emberek és a vállalatok egyaránt szeretik azt képzelni, hogy 18 éves kockafejek indítják őket a hálósobájukból. Ebben gyakran igazuk is van. A közvélekedés azonban lassan átalakul: a nyomozók mind gyakrabban állapítják meg, hogy a digitális támadásokat idegen államok kormányainak a megbízásából és hangszerelésében hajtják végre, amelyek magán közreműködőket vesznek igénybe, hogy a net felhasználásával kémkedjenek, szabotázsakciókat hajtsanak végre, és felforgató tevékenységet folytassanak. A Marriott szállodalánc elleni támadás állítólag a pekingi rezsim számára kémkedő kínai hekkerek számlájára írható.^[1] Peking tagadja a támadásokat – vagyis azt a rendkívül tipikus magatartást tanúsítja, melynek célja, hogy elhatárolja magát az idegen felségterületen végrehajtott törvénytelen akcióktól, és elejét vegye a nemzetközi közösség megtorló intézkedéseinek. Az állami támadások kiszervezése hekkerekhez, internetes trollokhoz és robotokhoz, röviden az állam alvállalkozóihoz, megkönnyíti bármiféle kormányzati részvétel tagadását.^[2]

A digitalizáció nem csak magánéletünket és munkás hétköznapijainkat tartja szilárdan hatalmában, a hadviselés is evolúciójának következő szakaszába lép át általa. A politika és a katonai erőalkalmazás számára az általános hálózatba szerveződés, folyamatos elérhetőségünk, a kommunikáció gyorsasága és az egyre intelligensebbé váló gépek egyfajta *szoft háború* hasznos eszközei. Lehetővé teszik, hogy nyomást gyakoroljanak államokra és azok lakosságára – még olyan stabil hatalmakra is, mint az USA –, de mégis alacsony szinten tartásuk a megtorlás és a helyzet tényleges, forró háborúvá való eszkalálódásának a kockázatát. Ez azonban, mint még látni fogjuk, nem zárható ki maradéktalanul. Az úgynevezett aszimmetrikus vagy hibrid fenyegetések, amelyek közé a digitális kémkedés, a szabotázs és a szubverzió tartozik, a háború megfizethető helyettesítőivé váltak.^[3] Mivel pedig a digitális támadások olcsóbbak, mint egy forró háború, egyre több állam – a gazdaságilag gyengébbek, kisebb katonai költségvetéssel, rosszabbul felszerelt csapatokkal rendelkezők, ugyanakkor pedig az új globális pozícióra törők is – buzgón kiveszi belőlük a részét, megzavarva ezzel a fennálló nemzetközi rendet és ennek korábbi egyensúlyát.

Ez az oka, hogy a 21. századi hadviselés számára egyre fontosabbá válnak az olyan univerzális technológiák, mint a kognitív gépekhez kidolgozott mesterséges intelligencia. Néhány nemzet világosan felismerte: a digitális technológiák nemcsak gazdasági hasznot hajtanak, hanem politikai és katonai fölényt is eredményeznek. Aki megtalálja a digitalizáció geostratégiai

bevetési lehetőségeit, vezető pozícióba juthat a nagyhatalmak újkeletű erőpróba-versenyében.

Az Egyesült Államok, amelynek vezető digitális hatalmi státuszát eddig senki sem kérdőjelezte meg, azt tapasztalja most, hogy egykor volt előnye rohamosan fogy, befolyása pedig, tetszik, nem tetszik, erőtől duzzadó felkapaszkodottak – különösen Kína – javára csökken. Amerika visszavonulása és az a vehemencia, amivel a vetélkedő hatalmak térben terjeszkednek, egy olyan új, ijesztő fegyverkezési verseny nyitányát jelenti, amely nem korlátozódik pusztán adatlopásra, szabotázsra és felforgatásra. A digitális fegyverkezési verseny azáltal, hogy az *internet of everything* (IoE, minden internetje) megjelenésével minden mindennel hálózatba kapcsolódik, hatalmába keríti a fizikai világot is, amely még okosabb lesz, mint az okostelefonjaink, okosházaink vagy okosautóink: elterjednek a harci robotok, a drónrajok, az intelligens implantátumok, a hálózatba kötött nukleáris fegyverek és az intelligens muníciót szállító hiperszonikus hordozóeszközök, amelyek akár óránként 33 ezer kilométeres, a hangét sokszorosán túlszárnyaló sebességgel néhány percen belül célba érnek.

Az *internet of everything* térnyerése áttekinthetetlenné teszi a 21. századi háború eszközeit, ezért csak tematikus válogatást adok belőlük.

Az **1. fejezet** azzal kezdődik, hogy az államok digitális módszerekkel kémkednek és szabotálnak. A hasonló, de nem állami szereplők – például bűnözők vagy terroristák – által önös érdekből végrehajtott műveletek kérdését tudatosan figyelmen kívül

hagyjuk, mert azon szeretnénk elgondolkodni, hogy vajon csakugyan háború-e az, amit mi különösebb megfontolás nélkül „cyberháborúnak” nevezünk. A háború nemzetközi jogi definíciója kifejezetten megköveteli előfeltételként, hogy államok közti cselekvésre kerüljön sor. Ha azonban az erőszak nem állami tényezőktől, például szabadságharcosoktól, felkelőktől, terroristáktól vagy állami megbízatással nem rendelkező privát hekkerektől indul ki, a szó szoros értelmében véve nem teljesül a fenti nemzetközi jogi követelmény.

Háborús vagy békeidőkben a hatalom kontrolljának állandó velejárója annak a bizalomnak az aláásása, amivel egy adott népesség a kormánya iránt viseltetik. Az efféle felforgatás mesterműve volt, ahogyan 2016-ban Moszkva koordinált támadásokkal ásta alá az amerikai elnökválasztási kampányt, amit Robert Mueller amerikai különleges ügyész vizsgált és ismertetett igen alaposan. A szubverziót a Facebook, a Twitter és társaik üzleti modelljei tették lehetővé. Az, hogy a 21. század információs tere miképpen osztja meg a társadalmat, és hogyan szolgál táptalajul a demagógok felemelkedéséhez, a **2. fejezet** elmélkedéseinek a tárgya.

A **3. fejezet** a virtuális világot elhagyva kilép a pusztító autonóm fegyverrendszerek fizikai valóságába. Nem csak Németország akarja 19. törvényhozási időszakának koalíciós szerződése értelmében 2021-ig törvényen kívül helyezni a letális, azaz emberélet kioltására alkalmas autonóm fegyverrendszereket: más államok is küzdenek ezeknek a fenyegető, új eszközöknek a szabályozásáért, amelyek a semmiből felbukkanva aktiválják *kill*

cycle-jukat (többelemlő csapásmérő akciósorukat), és emberi közreműködés nélkül képesek ölni. Betiltásukra azonban kevés az esély, azért is, mert Németország nem akarja szabályozni azt, ami saját felfogása szerint még nem létezik: azokat az autonóm fegyvereket, melyeknek döntő funkcióira az ember már semmiféle hatással nincsen. Lehetséges, hogy ekképpen a tilalom megvalósulása talán nem is a jogban, hanem az elektronikus hadviselés területén végrehajtandó magasabb szintű ellenintézkedésekben keresendő?

Akit digitális támadás ér, az lehetőleg bosszút akar állni.

„Ha egyszer egy ilyen hekker a kezem közé kerül, én kitekerem a nyakát!”, hallom józan, komoly programozóktól, akik digitális támadások következményeképpen újra meg újra plusz munkafeladatokkal szembesülnek. Emiatt aztán egyre több vállalkozás óhajt saját *hacking back* potenciált kialakítani. De vajon egyáltalán megengedett-e a visszahekkelés? Vajon a megtorlás csakugyan a valódi támadót éri utol – vagy netán egy vétlen szereplőt valamely szövetséges országban, akinek csak visszaélték a számítógépével egy támadás céljából? És ha mondjuk a *hacking back* megengedett, vajon a védekező fél készült egy eskaláció következményeire is? A digitális támadások elleni védekezés kényes politikai ügy, és komoly diplomáciai bonyodalmakat okozhat. Azt, hogy a nemzetközi jog hogyan áll a digitális idők védelmi kérdéseihez, a **4. fejezetben** taglaljuk.

Ha némelyik állam felismeri, hogy a digitális korszak technológiai a geopolitikájukat is támogathatják, technológiastratégiájukat is eszerint alakítják majd. Mint az **5. fejezetben** megállá-

pítjuk, a digitális stratégiákat illetően vannak különbségek a Nyugat, illetve Kína és Oroszország között. Különösen a mesterséges intelligenciát, a 21. század kulcstechnológiáját alkalmazzák eltérően az országok politikai rendszerük függvényében – itt a nagyobb gazdasági versenyképesség érdekében, ott a gazdasági szempontból releváns források politikai és katonai ellenőrzése céljából. A mesterséges intelligencia felhasználásának különbségei abból adódnak, hogy két eltérő rendszeralternatíva ütközik első alkalommal össze: a neoliberalizmus és a világuralomról szőtt kínai álom.

A két rendszeralternatíva között elhelyezkedő Európa kihívásokkal kénytelen szembenézni. Mit jelent vajon az új, ázsiai nagyhatalmi törekvés a mi európai földrészünk számára? Donald Trump Amerikája mindenestre nem száll síkra már Európa biztonságaért. A kontinens így még inkább csak magára számíthat a nyomással és a megosztó törekvésekkel szemben, amelyek a – közelebbi és távolabbi – Kelet részéről érik. Vajon képes-e Európa saját világpolitikát megfogalmazni és eszerint élni? Az új technológiák ebben segítségére lehetnek. Ezzel kapcsolatos elgondolások kis választékával szolgál a **6. fejezet**.

Amikor a politikai hatalom és a katonai erőszak kontextusában kezdtem foglalkozni digitális technológiákkal, nyomban a gondolkodás látszólag leküzdhetetlen akadályába ütköztem. Akinek jobb fegyvere van – mondaná az ember elsőre reflexszerűn –, az fog érvényesülni politikailag vagy katonailag. Csak lassan tárultak fel előttem a világrend szemünk előtt zajló rendkívüli átrendeződésének a politikai finomságai, és vált világossá

a folyamat jelentősége. Lélegzetelállító dolog történik, és arra vár, hogy észrevegyük, tudatosítsuk és tematizáljuk. A technológia pedig nem pusztán mellékszereplő, hanem az egyik, ha nem a legfontosabb kulcstényező abban, hogy miféle rend uralja majd ezt a mi digitális 21. századunkat.

[EGY]

A kód mint fegyver

A modern háborúk mások, néhány esetben olyannyira, hogy a régi NATO-kézikönyveket nyugodtan ki is dobhatjuk. (Judy Dempsey)

„A vádlott, Marcus Hutchins, más néven Malwaretech, tudatosan szövetkezett N. N. vádlottal, és megállapodott vele, hogy a következő bűncselekményt követik el az Amerikai Egyesült Államok ellen: egy éven belül számítógépes programokat, kódokat és parancsokat telepítenek szándékosan tíz vagy több védett számítógépre azzal a céllal, hogy kárt okozzanak.”^[1]

Így hangzik az Egyesült Államok Kerületi Bíróságának (Eastern District of Wisconsin, ügyiratszám 17-CR-124) vádja a 23 éves, brit állampolgárságú Marcus Hutchins, kártékony szoftvekről író blogger, az USA-beli Kryptos Logic cég munkatársa ellen.

A fiatalember 2017 augusztusában hazatérőben a Black Hat Briefings és a DEF CON hekkerkonferenciáról éppen a Las Vegas-i McCarran nemzetközi repülőtér előcsarnokában várakozott, hogy visszarepüljön Nagy-Britanniába, amikor őrizetbe vették, kikísérték a repülőtérrel, és az FBI Las Vegas-i kirendelt-

ségére vitték. Ott bűnszövetkezetben elkövetett törvénysértések vádjával szembesítették, nevezetesen, hogy megírta és néhány ezer dollárért eladta a Kronos nevű, bankok ellen bevethető trójai programot, amely bankszámlák hozzáférési adatait lopja el.

Amit a vádirat száraz jogi nyelven megfogalmaz – miközben csak állításokat tartalmaz anélkül, hogy bizonyítékokkal is szolgálna –, a fiatal programozó számára akár negyven év szabadságvesztést jelenthet. Azt állították ugyanis, hogy már tizenévesen „fekete kalapos” (black-hat) hekkerként ténykedett minden erkölcsi skrupulus nélkül harmadik felek megbízásából, mielőtt 2013 táján átállt a „fehér kalapos” (white-hat), azaz etikus, jó hekkerekhez. De nem voltak biztosak benne.

Nézőponttól függően tekinthetjük pikánsnak, zavarba ejtőnek vagy stratégiai szempontból észszerűtlennek az amerikai igazságszolgáltatás Marcus Hutchins elleni vádját, ugyanis épp ő volt az, aki – ráadásul csak 2017 májusában! – „vészkikapcsolót” talált és hozott működésbe a WannaCry zsarolószoftver programkódjában. Egyesek azt mondják, hogy teljesen véletlenül történt. Ezzel szemben az amerikai FBI azt állítja, hogy nem: csak azért ismerte Hutchins a leállító *kill switch*-et, mert részt vett a zsarolóprogram kifejlesztésében. Hónapokkal később aztán kiderült, hogy Marcus Hutchins, aki ártatlannak vallotta magát, az igazat mondta.

„Immár hivatalos – így a 2017 decemberi *Wall Street Journal* szalagcíme –, hogy Észak-Korea áll a WannaCry-os cybertámadás mögött”.^[2] Egy állam és hekkerei támadást intéztek számos más állam ellen.

Azt a vádpontot azonban, hogy ő a felelős a Kronos banktró-jai létrehozásáért, nem tudta megcáfolni Hutchins. 2019 áprilisában bűnösnek vallotta magát, elismerte, hogy ő írta és terjesztette a programot. Mindenesetre a többi vádpontot ejtették.

Biztonsági rések

„Hoppá, adatait zároltuk! Utaljon át 300 amerikai dollár értékű bitcoint a következő címre.”^[3] Ezt egy számjegyekből és betűkből álló hosszú farok követi – és jó néhány átutalás, amelyeknek a zsaroló a kedvezményezettje. A WannaCry zsarolószoftver 2017. május 12. hajnala óta rohamosan terjedt az egész glóbuszon, és 99 országot fertőzött meg – köztük Kínát és Oroszországot is, pedig ezeket az országokat szokták elsőként gyanúsítani a hekkertámadások „szerzőségével”. A kártékony szoftver a Microsoft operációs rendszerek egyik biztonsági részét használja ki, fontos adatokat zárol a megfertőzött számítógépen, és a hozzáférést csak egy bizonyos pénzösszeg kifizetése után teszi ismét lehetővé.^[4]

A szóban forgó Microsoft biztonsági rés hosszú ideig csak az amerikai nemzetbiztonsági hatóság, az NSA előtt volt ismeretes. Nemcsak az NSA, hanem más nyugati biztonsági szervezetek is gyűjtik a számítógépes programok biztonsági réseit – hekkersargonban *zero day*nek nevezik őket –, hogy szükség esetén betörhessenek a világ bármelyik számítógépébe. A biztonsági réseket normális körülmények között szigorú titoktartás övezi. A

titkolózás azonban gyorsan véget ért, amikor az NSA maga is egy adatlopás áldozatává vált. A Shadow Brokers nevű hekker-csoport, amely sikeresen rajtaütött az NSA-n, 2017 áprilisában nyilvánosságra hozta a Microsoft biztonsági réssel kapcsolatos lopott információt. Mindössze néhány napba telt, és a WannaCry megkezdte globális rablóhadjáratát.

A WannaCry először brit kórházaknak okozott kárt, azután a FedEx amerikai logisztikai vállalatnak, orosz bankoknak, az orosz belügy- és egészségügyi minisztériumnak, az orosz államvasutaknak és Oroszország második legnagyobb mobilhálózatának is. Németországban a vasút minden utasa számára gyorsan nyilvánvalóvá vált, hogy a Bahn AG is áldozattá vált: a német pályaudvarok menetrendi kijelzőin ugyanis szembeszökőn ott virított a zsaroló üzenet.

A Microsoft úgy tett, mintha aggódna, ugyanakkor viszont a gondatlan és könnyelmű felhasználókat tette meg társfelelőssnek a keletkezett kárért. Az NSA-n kívül ugyanis maga a Microsoft is rábukkant a biztonsági résre operációs rendszereiben – és már 2017 márciusában kiküldött egy szoftverjavítást felhasználóinak, amelynek be kellett volna zárnia a rést. Csakhogy felhasználók milliói mulasztották el frissíteni számítógépüket, s így módon támadhatók maradtak. Ami pedig még ennél is rosszabb: számos hatóság a veszélyeztetett állami infrastruktúrákhoz még ma is egy elavult, a szoftvergyártók által 2014 óta már nem frissített operációs rendszert használ – a Windows XP-t.

A 2017 májusi zsarolásos támadás arra is rávilágított, milyen nagy a tanácstalanság a szoftverrendszerek állami beszerzése során. A kritikus infrastruktúrák (közlekedés, energiaszektor, honvédelem, egészségügy, élelmiszerellátás, pénzpiacok vagy államigazgatás) digitalizálása döntés elé állítja a döntéshozót: *make or buy*? A harckocsik, atomerőművek vagy kórházak működtetéséhez a szoftvert vajon a Google-nál, az Amazonnál, a SAP & Co.-nál érdemes megvásárolni – vagy inkább házon belül kifejleszteni? A szakma itt *commercial off-the-shelf*-ről, tehát kereskedelmi kész-szoftverről, röviden COTS-ról beszél. Az első pillantásra a „bolti” beszerzés mindig olcsóbb, hiszen senki sem akarja újra elkészíteni, amit másvalaki már régen kitalált. Van azonban egy komoly akadály: a sztenderd-szoftver nagyon bizonytalan valami. Biztonsági rései világszerte gyorsan ismertté válnak, és ki is használják őket. A kritikus infrastruktúrák működtetése elleni cybertámadások pusztítók lehetnek, mindmáig nem léteznek ugyanis kötelező biztonsági szabványok.^[5]

Ami a dolgot ráadásul még inkább megnehezíti, az az, hogy a kritikus infrastruktúrák vagy katonai eszközök digitalizálását gyakran engedélyhez kötik, a műszaki terméktanúsítvány körülbelüli megfelelőjéhez. Rendes körülmények között egy effajta minősítésre egy részletesen specifikált célplatform, például egy fegyverrendszer, egy mérőrendszer vagy egy röntgenkészülék szoftverrel együtt végzett minősítése céljából kerül sor. Ha a célplatform frissítése céljából letöltik a szoftver újabb változatát, ugyanezen okból érvényét veszti a működési engedély is, valamint a többi olyan számítógépes program összes garanciá-

ja, amelyeket a korábban minősített célplatformmal integráltak. Az olyan idők tehát, amelyekben bennünket, fogyasztókat állandóan felszólítanak, hogy folyamatosan és valós időben újítsunk, nem jó idők az állam kritikus infrastruktúrainak működtetése szempontjából, azok ugyanis már húsz évesek vagy még ennél is régebbiek. Ez idáig nem tudni, kibogozható-e – s ha igen, miképpen – a gordiuszi csomó, ami annak a konfliktusnak a következménye, amely két inkompatibilis paradigma között áll fenn: a biztonsági okokból megkövetelt folyamatos frissítés és a közösségi használatú infrastruktúrák hosszú távra tervezettsége között.

De a Microsoft cég és vele a technológiai gigászok kitartanak amellett, hogy a számítógépes biztonság felelősséget ró a felhasználóra is, aki (morálisan) köteles számítógépét mindenkor harmonizálni a legkorszerűbb követelményekkel. Ami tehát a számítógép biztonságos működéséért viselt felelősséget illeti, ez ügyben a gyártók szerint a felhasználónak is vannak kötelezettségei – hiszen módjában áll, hogy saját működési biztonságát maga befolyásolja. A szoftvergyártók azonban nem vesznek tudomást arról, hogy a felhasználóknak, különösen pedig az államiaknak, nem áll módjukban minden további nélkül frissíteni egy tanúsítvánnyal rendelkező rendszert, a felhasználók pedig nagyon szívesen megfelelkeznek arról, hogy digitalizált infrastruktúrájuk valójában milyen intenzív karbantartást igényel.

Annak, hogy a digitalizált infrastruktúrák biztonságának kérdéseit nem lehet csak úgy lepasszolni a felhasználónak, az az alapja, hogy a vállalatok és a kormányok egyaránt erősen rá

vannak utalva harmadik felek kínálatára és szolgáltatásaira. Felhasználók milliói használják az olyan technológiai gigászok számítógépes felhőit, mint az Amazon vagy az IBM. Ezek biztonsága, működése, know-how-ja mindenestül attól függ, hogy a számítóközpontok üzemeltetői meg tudják védeni felhőiket a hekkertámadásoktól. Ez azonban sohasem sikerülhet maradéktalanul. Minden szoftverködnek, a számítóközpont-belieknek is, vannak hibái vagy biztonsági rései: úgynevezett *bug*jai. A szoftverhibák, amelyek lehetővé teszik a hozzáférést a számítógépekhez, aranyat érnek, s amíg a nyilvánosság még nem tud róluk, és még senki nem foglalkozott egyetlen napig sem a korrekciójukkal (innét a *zero day* elnevezés), olykor akár hatszámjegyű dollárösszegekért cserélnek gazdát.

A Microsoft ez okból érthető szemrehányásokkal illeti az NSA-t. Az amerikai állam gyűjti a döntő fontosságú számítógépes programok biztonsági réseit, de maga sem tudja titokban tartani őket. Az adattolvajok kezében a biztonsági résék pusztító fegyverekké válnak, mondja Brad Smith, a Microsoft főjegősa – sőt, tömegpusztító fegyverekké. Egyetért ezzel Michael Rogers, az NSA volt vezetője is. A számítógépes férgeket és vírus-szoftvereket, indítványa szerint, a nemzetközi hadijog hatáskörébe kellene utalni: „a cyberfegyverek csak egy újabb technikai lehetőséget jelentenek, hogy néhány esetben ugyanazokat a károkat idézzék elő velük, mint a hagyományos fegyverekkel.”^[6]

„A Microsoft biztonsági résék ellopása az NSA-nél összevethető azzal, mintha az USA haderejétől néhány Tomahawk manőverező robotrepülőgépet lopnának el” – fogalmazza meg

végkövetkeztetését hasonló határozottsággal Brad Smith.^[7] „A legutóbbi támadás egy abszolút akaratlan és rendkívül nyugtalanító szövetségre vall a világszintű biztonsági fenyegetések két legsúlyosabb formája, az állami akciók és a bűncselekmények között.”^[8]

Két út a hatalomhoz

Amikor a 21. században olyasmi válik fegyverré, ami nem tartozik a korábbi évtizedek klasszikus fegyverarzenáljába, mert újfajta technikát képvisel, ideje reflektálnunk rá, hogyan változik meg a háború természete a digitalizáció révén, és hogyan kérdőjeleződik meg alapvetően a háborúval és békével kapcsolatos felfogásunk.

A háború az ember alaptapasztalatai közé tartozik, és „olyan régi, mint az emberiség dokumentált története”^[9]. A katonai erőszak okai sokfélék. A legerősebbek és legrátermettebbek bizalmatlanságból vagy a saját tehetetlenségüktől való félelmükben törnek hatalomra.^[10] A szociáldarwinizmus mellett gazdasági kényszerek, territoriális igények, katonai-stratégiai megfontolások vagy technikai fejlesztések azok, amik kiváltják a „háborúnak” nevezett eseményt, igen sajátos szociális, egyben pedig jogi viszonyt hozva létre az emberek között. A háború alapvető szociális rendszer, „a társadalom alapvető strukturáló ereje politikai ideológiák és jogi rendszerek fenntartása érdekében”^[11].

A háború, amint egykoron Carl von Clausewitz (1780–1831) vezérőrnagy, katonai teoretikus a 19. század elején megfogalmazta, „a politika folytatása más eszközökkel”^[12]. Az érvényes nemzetközi hadijog szerint a politika efféle folytatására úgy kerül sor, hogy az egyik állam hadat üzen egy másiknak. Ezzel a háború jogilag államközi folyamatként definiálódik. Egy efféle államközi konfliktus esetén a nemzetközi jog nemzetközi fegyveres konfliktusról beszél – nemzetek közötti fegyveres konfliktusról.

A politika és a háború aszimmetrikus páros, egy *vagy-vagy*, de mégis elválaszthatatlannak tűnnek egymástól. Mindkettő befolyást gyakorol az emberek akaratára,^[13] és mindkettő ugyanazt a célt követi: emberek rábírását egy bizonyos viselkedésre. Módszereik azonban alapvetően különböznek: a háború a katonai erőszak eszközeivel dolgozik, a politika a meggyőzés pusztá erejével.

A veteránok is állítják, hogy a háború és a politika világosan megkülönböztethető egymástól. A különbséget, mint mondják, az eszköz megválasztása jelenti, úgyhogy a háború nem egyszerűen más névvel illetett politika.^[14] Ha az ember egy kés pengéjét érzi a torkán, az egészen másféle meggyőző erővel bír, mint egy véleményformálást célzó politikai vita. Mert igaz ugyan, hogy a háború sem jogilag szabályozatlan zóna, hiszen az emberiség alapelveit mindenkor figyelembe kell venni (de mégis nagyon gyakran lábbal tiporják őket), a háborúban valóban az erősebb joga érvényesül, semmilyen életet nem kímél-

ve. Egy hadviselő büntetlenül megölhet egy másik hadviselőt, mert egy ilyen emberölés nem jár semmilyen szankcióval.

Politikai hatalomgyakorlás idején más szabályok érvényesek, és egy másik ember megölése mindig büntetendő. Ám a jogi szankciókkal való fenyegetés nem jelent kényszert az alárendelődésre, mint egy háborús konfliktus idején. A politikai uralom normatív rendszerei sokkal inkább szabadságot szavatolnak az így uraltak számára, ugyanis mindenki eldöntheti, hogy követi-e az érvényes normákat, vagy inkább vét ellenük. Amiben tehát a politika reménykedik, az az uraltak önkéntes alárendelődése – akkor lemondhat a fizikai kényszerről. Ezért Hannah Arendt, a 20. század nagy politikai teoretikusa is határozottan megkülönbözteti a (politikai) hatalmat és a (katonai) erőszakot: „Hatalom és erőszak egymásnak ellentéte: ahol abszolút módon uralkodik az egyik, nincs jelen a másik.”^[15] Ezt a dichotómiát, ami lényegében Goethe Rémkirályának *„eljössz, vagy erővel viszlek el”* (ford. Vas István) sorára redukálható, lényegében még ma is számos politikus és katonai stratégia vallja.

Minthogy azonban a politikában sem maradnak a dolgok az egyszer elért állapotban, „mivel az összesség akarata nem előre létrehozva adott egyszer s mindenkorra (...), a hatalmat előbb gondosan ki kell alakítani, újra és újra tagolni kell, (...) az állam tisztán mechanikus működése kezdetben eleve kizárt”,^[16] a politika is kénytelen újra és újra elnyerni és legitimálni a hatalmat. Ha a meggyőzés és normaadás politikai folyamata nem jár sikerrel, a hatalom nem kevés birtokosa mindkét irányba elindul, és a politikai hatalom elnyerése érdekében saját meggyőző

erején túl a katonai erőszak alkalmazásának technikai eszközeit is beveti. Ahogyan Mao Ce-tung cinikusan összefoglalta: „A hatalom egy hordó puskaporból ered.”^[17] „Minden politika hatalomért folytatott harc, a hatalomgyakorlás végső formája pedig a [katonai] erőszak”, ismeri el ezért abszolút találóan a szociológus C. Wright Mills is.^[18]

Elkötelezettség a béke iránt

A békeszerződésekkel a háborúk véget érnek. A béke a katonai teoretikusok szerint egy háború befejeződése, s így megcélzott végállapot. A béke és a háború, úgymond, váltakozik egymással; olyan ciklust alkot, melyben háborúra béke következik, békére pedig háború, még ha a ciklusok jelentős időbeli szabálytalanságot mutatnak is.

A mi európai felfogásunk szerint a béke érték, amit meg kell őrizni, és még stabilabbá kell tenni, hogy ezáltal lehetővé váljon a társadalmi haladás. A békének, így hisszük mi, európaiak, mindig még nagyobb békéhez kell vezetnie. Az európai béke az Európai Uniónak az a politikai eszméje, amiért 2012-ben Nobel-békedíjjal tüntették ki.

Ma, néhány évvel később és olyan konfliktusok után, mint a szíriai, jemeni vagy az Iszlám Állammal vívott volt, nyilvánvalóan látszik, hogy a béke elmélyítésének célja alighanem igen csak európai eszme. Így a katonai erőszak elutasítása is a hadviselés kulturálisan meghatározott, etnocentrikus megközelítése.

Más kultúrákra ugyanis egyáltalán nem érvényes, ami iránt Európa olyannyira elkötelezettnek érzi magát. Ezt Angela Merkel harmadik kormányának külügyminisztere, Sigmar Gabriel az 54. Münchener Biztonsági Konferencia alkalmával így fogalmazta meg: „Egyetlen vegetáriánusként átkozottul nehéz dolgunk lesz a húsevők világában.”^[19]

Pedig ha az ember a józan ész alapelveit követi, a békét tartósan meg kell teremteni, vélekedett már Immanuel Kant is *Az örök béke* című 1795-ös esszéjében. Kant művének fénye még a 21. századba is átragyog, mert alapját képezi az Egyesült Nemzetek Chartájának, amely nagyon határozottan megfogalmazza az erőszak tilalmát.

A józan észnek ugyanerre a lapjára tett az Egyesült Államok a II. világháború végén: arra, hogy a háború nem maradhat fenn kereskedelem mellett. Vagy másként megfogalmazva: aki vásárol, az nem lő. Mit sem törődve az ezermilliárdos költségekkel és befektetésekkel, az amerikaiak késznek mutatkoztak, hogy magukra öltse a globális rendfenntartó hatalom szerepét. Biztosítani akarták, úgymond, „hogy virágozhasson a világkereskedelem, és hogy az Egyesült Államok ne keveredjen megint olyan nagy, regionális, államközi konfliktusokba, mint a két világháború volt”,^[20] akkor is, ha gazdaságilag nem válna mindig az USA előnyére.

Az az elképzelés, miszerint a háborús állapotok véget érnek, és átadják helyüket a békének, még ma is sok embert lelkesít. Amikor az erőszak véget ér, és béke uralkodik – így remélik –, kibontakozhat a politikai hatalom. Csakhogy már Hannah

Arendt is megállapította: a két világháborúra a hidegháború következett a maga fegyverkezési verseny és elrettentés jellemezte politikájával, valamint a katonai-ipari komplexum megteremtésével az Egyesült Államokban.^[21] Aki Arendttől inspirálva tovább viszi a gondolatot, kénytelen konstatálni: a hidegháborúra, amelyben hallgattak az atomfegyverek, a terror elleni háború következett, most pedig a „cyberháború”. Akkor hát az az állapot, amelyben nap mint nap élünk, nem teljes béke, csak egy naponta fenyegetéseknek kitett nyugalmi fázis, amely soha sem lehet biztonságban az eszkaláció veszélyével szemben. Akkor hát közvetlenül ugyan nem vagyunk kitéve fizikai erőszaknak, de állandóan együtt élünk egy diffúz fenyegetéssel és azzal a lehetőséggel, hogy az erőszak egy napon váratlanul, kézzelfogható formában manifesztálódik, és bármelyikünket elérheti. Akkor hát a hatalmat és az erőszakot, a békét és a háborút mégsem tudjuk élesen elhatárolni egymástól. Ehelyett a két szituáció közti tartósan zavaros állapotban élünk – egy hibrid helyzet kontinuumában.

A gondolat, hogy a háború és béke dualizmusának helyébe egy állandó folyamat léphet, amelyben nem határolhatók el egymástól világosan a különböző állapotok, a kezdet és a vég, a barát és az ellenség, a hadviselő és a nem hadviselő, különösen a németek és európai szomszédai számára nehezen felfogható. Ők keservesen megtapasztalták, hogy a háború semmiféleképpen nem célravezető. Az erőszak ellenerőszakot vált ki; a háború pedig mérhetetlen költségekkel és elmondhatatlan szenvedéssel jár. Mindenekelőtt az 1968-as nemzedék szegült szembe a

háborúval. A lázadás következményeiért még ma is hálások lehetünk: a polgári jogok, a demokrácia és a jogállam éppúgy felvirágzott, ahogyan a gazdaság és az innovációs potenciál a nyugati világban.

Elmélyült és szerteágazó globális kapcsolatokat, maradéktalanul az emberiség javát szolgáló technológiákat, jobb egészséget, hosszabb életet, mindenekelőtt pedig több demokráciát és a nemzetek közti egységes világkereskedelem következtében a háborúk helyébe lépő békét ígért Kalifornia technológiai elitje is.^[22] Ma már valószínűleg aligha hinne nekik bárki is. Valójában minden egyes technológiai korszak saját fegyvertechnikai fejlesztéseket és hadviselés-formát vezet be.^[23] Az I. világháborút az ipar dimenzióiban vívták, a II. világháborúban Németországot Josef Goebbels propagandaháborúja készítette ujjongásra, amelynek eszközei az első rádiók voltak, azóta pedig, hogy a hidegháború idején rendszerbe állították a nukleáris fegyvereket, az egész emberiséget fenyegeti a pusztulás, ha be találják vetni őket.

Közben hatásosan bizonyosodott, hogy a digitalizáció demokratikus államok elleni támadásokat tesz lehetővé. Még csak a digitális korszak kezdetén állunk, és nem egészen értjük, hogy a társadalmi szerveződés milyen formáit tartogatja még számunkra, ha meghatározatlan ellenfelek titokban vagy nyíltan, névtelenül vagy felismerhetően megfertőzik, manipulálják vagy károsítják az életünket, a gazdaságunkat vagy a kormányzatainkat. És még ha nem akarjuk is eljátszani a digitalizáció nyújtotta esélyeinket: marad bennünk némi rossz érzés.

Az állam és a hatalom

A háborúval és a politikával kapcsolatos felfogás alapjául – tekintet nélkül arra, hogy különböző szakaszoknak vagy egyetlen kontinuumnak tekintjük-e őket, és hogy a nemzetközi hadijog eddigi interpretációjához ragaszkodunk-e – az az elterjedt elképzelés szolgál, hogy egyedül az állam rendelkezik hatalmi monopóliummal. A szuverén államok hatalmi monopóliuma volt az, ami az utóbbi hetven évben a biztonság megteremtését szavatolta.^[24]

„A hatalmi monopólium – foglalja össze a Münchener Biztonsági Konferencia vezetője, Wolfgang Ischinger nyugalmazott nagykövet – azt jelenti, hogy az állam előírja polgárainak, kinek szabad erőszakot alkalmaznia.”^[25] Az erőszak alkalmazásának legitimációval kell rendelkeznie, és az állam ellenőrzése alatt kell állnia. Ez a jogállam elvének központi követelménye. Egyedül emiatt „válíkat lehetségessé a politikának az a formája, amelyik számunkra magától értetődik”^[26].

A háborúban a haderő az, ami felhatalmazást kap az erőszak alkalmazására. Ez megfelel a társadalom háromszögmodelljén belüli összefüggéseknek, a társadalom, az állam és a fegyveres erők hármasságának, ahogyan ezt a katonai teoretikus Clausewitz elgondolta. Még napjainkban is sok állam támaszkodik erre a hármas kapcsolatra. A választások során a németek is lemondtak az uralkodói hatalomról hivatásos politikusaik javára, s ezzel egyúttal meg is bízták őket, hogy őrizték meg a nemzet békéjét, és mint közjóról, gondoskodjanak a belső és a külső biz-

tonság fenntartásáról. A német kormány a maga részéről ezt a feladatot a prioritásokat mérlegelve átadja a Bundeswehrnek, a rendőrségnek és a többi biztonsági szervezetnek. A katonák, esetleg a rendőrök azok, akik meghatározott jogi feltételek mellett jogosultak erőszakot alkalmazni, például mert fegyvert vihetnek.

Az állam hatalmi monopóliumának kontextusába illeszkedik továbbá, hogy nemcsak a háború, hanem a diplomácia is államok közt zajlik.

„1945-ben, az ENSZ alapításakor még abból indultak ki, hogy a kormányokat féken kell tartani, azoknak pedig a nemzetközi joghoz kell tartaniuk magukat”, folytatja az állam hatalmi monopóliumával kapcsolatos gondolatmenetét Wolfgang Ischinger. [27] Az államok erőfeszítései az ENSZ-ben, az állandó leszerelési konferencián Genfben, vagy a Münchener Biztonsági Konferencián csakugyan elvezetett az államközi háborúk számának csökkenéséhez, mert a II. világháború során küldték az érvényes hadijog szerinti utolsó hadüzenetet. Csakhogy a napi hírek egymásik valóságról beszélnek. A háború, akár egy vírus, mutációkat hoz létre túlélése érdekében. Az utóbbi évtizedekben a háborúk már a digitális fejlődés nélkül is „újfajta háborúkká” változtak – ahogyan Herfried Münkler német politológus nevezi őket. [28] Wolfgang Ischinger ezt a jelenséget is össze tudja foglalni egy szikár tételbe: „A 21. század konfliktusai között egyetlen egyet sem találni, amely megfelel az államközi háború mintájának; mindig egyes államokon belüli konfliktusokról van szó.” [29]

A II. világháború utáni valamennyi háborút formális hadüzenet nélkül vívták – a koreai háborútól a vietnami háborún át a szíriaiig. Igaz ugyan, hogy már helyettesítő jellegük miatt is nagy nemzetközi jelentőséggel bírnak, ezzel együtt megállja a helyét a kijelentés, mely szerint „a Genfi Konvenció értelmében *nem* minden nemzetközi dimenzióval rendelkező fegyveres konfliktus” számít nemzetközi fegyveres konfliktusnak.^[30] A nemzetközi jog tehát egyértelműen különbséget tesz egy államközi konfliktus és más, nem nemzetközi fegyveres konfliktusok,^[31] vagyis az olyanok között, amelyeknek államközi jellegét nem nyilvánítják ki, és mégis határokon átnyúló módon vívhatják őket.^[32]

Mármost Herfried Münkler az „újfajta háborúkat” oly módon definiálja, hogy ezeket „nem kormányok, hanem nem állami szereplők váltják ki”. Utóbbiak ennek megfelelően nem nyílt harcot folytatnak, hanem az aszimmetrizálás stratégiáját követik”.^[33]

Jelenleg még nem nyilvánvalóan ez a helyzet, de közelítünk ahhoz, ami a digitális 21. század konfliktusait is jellemzi: hogy a digitalizáció egyes kis csoportok vagy konvencionális fegyverzettel gyengén felszerelt államok számára lehetővé teszi, hogy még magasan fejlett nemzeteket is jelentős sikerrel, nagy pusztító potenciállal, ugyanakkor csekély költségráfordítással megtámadhassanak. Észak-Korea képes az egész világot digitális eszközökkel zsarolni, holott a gazdasága gyenge, energiaellátásában könnyen következnek be zavarok, és az ország egészében alig működik digitális integráció.

A digitális cselekvés lehetőségéből – rendelkezzenek bár vele államok vagy nem állami szereplők – következik, hogy a nemzetközi rend, illetve az egyes államok hatalmi monopóliuma egyaránt sebezhető. Ha valaki utánanéz, kik az új évezred háborúinak szereplői, és hogy milyen eszközöket alkalmaznak e konfliktusokban, akkor el kell ismernie, hogy azok a háborúk, amelyeket mi nemzetközi jogi szempontból szabályoztunk, történelmi kifutó modellek lettek, és a clausewitzi felfogás elavult. [34]

Noha az államok a digitális érában is megtesznek mindent hatalmi monopóliumuk megőrzése érdekében, s már csak ezért is ragaszkodnak a nemzetközi hadijoghoz, csorbult a hatalmuk. A 21. században olyan támadásoknak vannak kitéve, amelyekkel nem számolnak, de amelyek pusztító következményekkel járnak.

Egyetlen svájci banki alkalmazott, aki ügyféladatokat másolt egy CD-re, majd továbbértékesítette őket idegen kormányoknak, többek közt Franciaországnak, Németországnak és az Egyesült Államoknak, mindörökre ellehetetlenítette a svájci banktitkot, és végleg elavulttá tette Svájc egykoron igen jól jövedelmező üzleti modelljét. [35] Az interneten szabadon áramlanak a szoftverködök, amelyekkel magánemberek nemcsak hogy támadásokat intézhetnek kritikus fontosságú állami infrastruktúrák ellen, hanem például 3D-nyomtatók segítségével fegyvereket is elő tudnak állítani. Az online platformok egészen kicsiny csoportok, köztük például terroristák (amilyen az Iszlám Állam) számára is lehetővé teszik, hogy konfliktusokat stratégiai kommunikáció-

val és narratívákkal kövessenek, s ezáltal a globális közösség kommunikációs terét zavaró képekkel telítsék valós időben. Az internetes fórumok lehetőséget teremtenek harcosok toborzására a világ minden részéről, és azok YouTube-videókkal történő motiválására. A Twitter segítséget nyújt forradalmak szervezéséhez és kormányok megdöntéséhez – még ha az efféle felkelések a *failed state*, a működésképtelen állam állapotához vezethetnek is, ahogyan ezt a 2011-es arab tavasz líbiai történései igencsak egyértelműen példázták. Mesterséges intelligenciák ingyenes nyílt forráskódja rosszhiszemű szereplőknek is kezébe adja a lehetőséget, hogy algoritmikus fegyvervezérléseket dolgozzanak ki – még ha a gyakorlatban ez nem is ennyire egyszerű. Ami igaz a nem állami szereplőkre, azoknak a kisállamok ambícióira is igaz, amelyek eddig pusztán csak alárendelt szerepet játszottak a nagyhatalmak, a nukleáris hatalmak, a G4, G7 vagy G20 államok mellett. Ma minden állam, függetlenül attól, hogy nagy- vagy középhatalom, domináns szerepet játszhat bizonyos területeken.^[36] A digitalizáció minden esetben az egykori gyengék hatalomhoz jutását vonja maga után, akiket a digitalizáció új erővel ruház fel, ami azonban – feltéve, hogy Herfried Münkler elemzése tizenöt év elteltével még mindig megállja helyét – a nukleáris hatalmak katonai erejével összevetve nem szimmetrikus. A digitális fejletlenség, vagyis az, hogy számos funkciót továbbra is analóg technika lát el, akár támadások ellen is védelmet nyújthat. Ezért tehát az, ha valaki a legmodernebb technológiákkal szerelkezik fel, egyaránt jár nagy felelősséggel és magas kockázattal.

A világrend aszimmetriája

Az információelméletben a „szimmetria” és „aszimmetria” szónak mindazonáltal más a jelentése, mint amiben Herfried Münkler az újfajta háborúk magyarázata során használja őket. Miközben az aszimmetriát jelentős mértékű rend jellemzi, a szimmetria semmiféle információt nem tartalmaz. Alkalmazzuk most ezt az elméleti megfontolást a világrendre.

Tegyük fel, hogy mindenki egyenlő hatalommal bír, mert ugyanazzal a hozzáféréssel rendelkezik adatokhoz, információkhoz és tudáshoz, mint mindenki más. Ez neki és mindenki másnak ugyanolyan potenciált biztosít, hogy tegyen valamit, és hogy cselekedjék. A cselekvési potenciál egyenlően oszlik el. Senki nem élvez előnyt, senkit sem sújt hátrányos megkülönböztetés. A rend vagy a hatalmi monopólium makroszkopikus struktúrái nem állnak fenn. Ha egy egyéni szereplő, illetve döntései és akciói körül rövid időre mégis finom struktúrák alakulnak ki, ezek mikroszkopikusan aprók lesznek, és gyorsan szét hullanak.

Ha megpróbálnánk függvény formájában vizualizálni az ilyen egyenlő eloszlást, illetve a hatalom szimmetriáját, egy téglalap hosszabbik oldalához hasonló egyenes vonalat kapnánk, amelyen fel lenne tüntetve minden egyes szereplő hatalmának mértéke. Egy ilyen egyenes semmiféle információt nem közöl. Ezzel maximális entrópiát reprezentál, az információtartalom mértékét, avagy a teljes struktúranélküliséget, mindenféle vo-

natkoztatási pont nélkül. A szimmetria, mondják ezért az információelmélet művelői, semmiféle információt nem hordoz.

Ha visszatekintünk a 20. század második felére, éppen a hatalomnak a polgárok és az állam közötti, valamint az egyes államok közötti megoszlásának aszimmetriája volt az, ami a nyugati társadalmakban a békét, a biztonságot és a rendet biztosította. Képzeljük el továbbá, hogy az egyenes vonalon eloszló hatalom egy egyetlen kiugró csúcsot produkál, amely egy olyan államot reprezentál, amely globális rendfenntartóként lép fel, mivel hatalmat koncentrált a kezében. Ez az unipoláris eloszlású hatalom, amit egy domináns állam gyakorol más államok felett, a rendszer többi szereplőjétől vonódik el. Ennek az egyetlen globális rendfenntartó hatalomnak a javára történik felhatalmazás, méghozzá úgy, hogy a többiek hatalma csökken, éspedig abban az értelemben, hogy óriási hatalmi szakadék fog tátongani a globális rendfenntartó hatalom és a gyengébb államok, de a rendfenntartó hatalom és saját polgárai között is.

A berlini fal 1989-ben bekövetkezett leomlása óta néhány éven át az USA testesítette meg azt az államot, amely hegemon hatalomként a Föld minden zugában azzal a kinyilvánított szándékkal lépett fel, hogy technológiailag, gazdaságilag és kulturális tekintetben vezető szerepet játsszon. Azokon a helyeken, ahol katonai támaszpontokat tartott fenn, előfordulhatott, hogy az USA imperialisztikus vonásokat is öltött. Rendszerszempontról vizsgálva az Egyesült Államok hatalma és a hatalmi szakadék volt a garanciája annak a stabil világrendnek, amelyben az európaiak a csatlósállamok szerepét vették át, és Amerika

perifériáján, az Atlanti-óceán másik oldalán tekintetüket tudatosan az Egyesült Államokra függesztve tevékenykedtek.

Az európaiak Amerika irányítói hatalmának potyautasai-ként, haszonélvezőiként^[37] viselkedtek: azokból a katonai konfliktusoktól, amelyek valószínűsíthetően kevésbé érintették őket, kimaradtak, és teljességgel az Egyesült Államokra bízta magukat. Amerika haszonélvezőiként ott is megjelentek, ahol az amerikaiak dollár ezermilliárdokat fektettek digitális lehetőségekbe, hogy előre vigyék a digitalizációt. Európaiakként ők maguk miért is adtak volna ki pénzt digitális kulcstechnológiákért, ha már egyszer valaki megtette? Minek fejlesztették volna ki újra saját maguk azokat a dolgokat, amelyeket a Szilícium-völgy oly ragyogóan a piacra dobott – az okostelefonoktól az operációs rendszereken át a közösségi médiáig és a hatalmas keresőmotorokig? Az amerikaiak, és áll ez Donald Trumpra is, ma úgy gondolják, ők voltak, akik az internetet feltalálták.^[38]

Időközben Európa számára is világossá vált, hogy az Egyesült Államokhoz fűződő külkapcsolatainak utolsó húsz esztendejében mennyire ráhagyatkozott az USA digitalizációs erőfeszítéseire és ezermilliárdos nagyságrendű beruházásaira. Mivel úgy tűnik, hogy Amerikának a stratégiai partnereivel kapcsolatos viselkedése alapvető változáson megy át, Európa hirtelen azon veszi észre magát, hogy kemény technológiai versenyben kell helytállnia, amely cselekvő szerepbe kényszeríti.

Következésképpen a hatalomeloszlás aszimmetriájának megvannak a maga előnyei és hátrányai, a vezető nagyhatalom számára is. Globális rendfenntartó hatalma Washingtonnak

nem mindig járt materiális haszonnal, mert hatalmas pénzügyi ráfordításokat igényelt, kereskedelmi deficitekhez és az állam eladósodásához vezetett, ugyanakkor évtizedeken át lehetővé tette számára a béke és a háború közben tartását. Annak a világrendnek, illetve -rendszernek, amelynek hatalmi központjában Amerika állt, csekély volt az entrópiája, információtartalma ezzel szemben magas, mert ennek a világrendnek a globális rendszere olyan tulajdonságokkal rendelkezett, amelyek lehetővé tették, hogy viselkedését meglehetősen biztonsággal előre lehessen jelezni. A rendfenntartó politika efféle attribútumai közé tartoztak a 20. század második felében a multilaterális kereskedelmi egyezmények éppúgy, mint a Kereskedelmi Világszervezet vagy a Világbank. Emberek létrehozta rend volt ez, és megmutatkoztak a hatásai: politikai-gazdasági-jogi ösztönzőket alkalmaztak, a rendszer pedig az elvárt módon reagált.

A világrend megjósolható működésére még akkor is támaszkodni lehetett, amikor két nagyhatalom, a Szovjetunió és az Egyesült Államok egymás közt két – egy nyugati, demokratikus-kapitalista, és egy keleti, kommunista-tervgazdasági – tömbre osztotta fel a világot. Szemléletesen szólva: az egyenlőképpen megosztó hatalom egyenesén ekkor két, hatalomért viaskodó csúcs keletkezett. A hatalom eloszlása bipoláris volt. Miközben az Egyesült Államok leginkább vezető hatalomként igyekezett fellépni, és *soft power*jére, puha eszközökre épített hatalmára támaszkodott, a Szovjetunió egyértelműen imperialista módon viselkedett, a Varsói Szerződés csatlósá államait erőszakosan és katonai eszközökkel nyomta el.

Az, hogy a II. világháború vége után ennek ellenére nem került sor nyílt, államközi háborúra a két nagyhatalom közt, a két tömb közötti stratégiai egyensúlynak volt köszönhető. Az elrettentésre épülő egyensúly John Nash amerikai matematikus játékelméleti koncepcióját hasznosította, s végül az elrettentés politikájába torkollott.

Egy forró háborút csak akkor volna érdemes megvívni – hangzott a feltételezés még a nyugat–keleti konfliktus tetőpontján is –, ha a békekötés is kifizetődne, aminek során a győztes a saját feltételei szerint diktálná a békét. A hidegháború idején azonban egy ilyen győztes által diktált béke semmiképpen sem volt biztosra vehető. Nyilvánvaló volt, hogy bárki győzne is, egy nukleáris ütésváltás mindkét tömb számára a véget jelentené. Az Egyesült Államok ellen elsőként intézett szovjet nukleáris csapás Moszkva számára igazából csak akkor fizetődött volna ki, ha saját lakosságára nézve nem járt volna hátrányokkal. Ebből azonban a szovjetek egyáltalán nem indulhattak ki. A fenyegető szovjet nukleáris első csapással számolva ugyanis az amerikaiak gondoskodtak arról, hogy második csapás mérésére való képességük egy megsemmisítő támadást követően is megmaradjon. A nukleáris második csapás – így hangzott az amerikaiak elrettentő célzatú fenyegetése – nukleáris sivataggá változtatná a Szovjetuniót; így hát egy forró háború nem szolgált a hidegháború valódi alternatívájaként.

Az elrettentés mindazonáltal a remélt hatással járt. Ami matematikai számítások eredményeképpen és egyáltalán nem véletlenül jött létre, bekövetkezett: a két nagy tömb között stratégiai

ai egyensúly uralkodott. A két nagyhatalom egyike sem mert közvetlen, katonai kihívást intézni az ellenfélhez. A két tömb makroszkopikus struktúrája, fegyverkezési versenyt és elrettenést alkalmazó politikája kézben tartható volt, és társadalmi stabilitást biztosított, igaz, csak ritkán enyhült a polgároknak az a kellemetlen érzése, hogy a Föld állandóan teljes megsemmisülésnek szélén egyensúlyoz: szorongásuk és félelmük húsvéti békemenetekben és békemozgalmakban nyilvánult meg.

2001 óta az Egyesült Államok technológiai és katonai fölénye ellen senki sem intézett komoly kihívást, még a terroristák sem – ennek ellenére érezhető: a digitális fejlődés következtében fokozatosan kezd változni a helyzet. A mind nagyobb mértékű hálózatosodás egyre több szereplő számára biztosít mozgásteret és lehetőségeket, és a hatalom, valamint az erőszak olyan hatékony eszközeit adja kezükbe, amelyek a 20. században még csak államokkal kapcsolatban jutottak eszünkbe.^[39] Elkerülhetetlen tehát, hogy a digitalizáció éppoly alapvetően megváltoztassa majd a geostratégiai hatalmi viszonyokat, ahogyan ez már az első ipari forradalom idején is megfigyelhető volt.^[40]

Ma az új hatalmasok között Kína vagy a putyini Oroszország mellett nem csak más államok is találhatók, de még egyének, cégek vagy olyan kisebb-nagyobb szervezettségű képződmények is, mint a terroristacsoportok vagy a hekkerszervezetek. Az új hatalmasok közt maguk a technológiaszolgáltatók állnak az első helyen. Ha az Apple az első vállalat, amelynek piaci kapitalizációja átlépi az ezermilliárd dolláros küszöböt,^[41] akkor, legalábbis pénzügyi tekintetben, hatalmasabb, mint a Föld legtöbb

állama. Ezek a magántulajdonú tőkés szervezetek rendkívüli hatalommal rendelkeznek, ugyanakkor átlátható állami ellenőrzés alatt állnak. Utópiájuk azonban az, hogy adatok, adatelemzés és a mesterséges intelligencia segítségével meghódítsák a világot.

A hatalommegosztás kérdését csak ki fogja élezni Amerika önkéntes politikai visszavonulása a globális rendfenntartó hatalom szerepéből. Az *America First* jelszó nem Donald Trump tálmánya. Először 1916-ban Woodrow Wilson demokrata követői jelentették ki,^[42] de a republikánus Trump-adminisztráció olyan lázas becsvággyal valósítja meg, hogy tartani lehet az *America Alone*-tól: „A mi hitvallásunk az amerikanizmus, és nem a globalizmus lesz.”^[43]

Az izolacionista politika nem marad következmények nélkül. Miközben egy magas rangú NATO-diplomata bevallja: „Az amerikai vezetés nélkül el vagyunk akadva”,^[44] Donald Tusk, az Európa Tanács soros elnöke jóval haragosabban ezt twitterezi Donald Trumpnak: „Tisztában vagyunk vele, hogy ha Önnek segítő kézre van szüksége, a karja végén találja meg.”^[45]

Egy globális rendfenntartó hatalom visszavonulási stratégiája rendszerszintű törésekhez vezet majd, amelyeknek súlyosak lesznek a következményei. Ha a rendező struktúrák nem tartanak ki, hanem széthullanak, és a bizonytalanságot még tovább fokozza a digitalizált társadalom felaprózódottsága és mikrostrukturáltsága – mivel nagyszámú, hatalmi igénnyel fellépő szereplő nő fel vagy erősödik meg –, nehezen megjósolható, milyen környezeti dinamika alakul ki. Megbízható információk híján

azonban fokozódik az entrópia, nő a rendezetlenség és a strukturálatlanság, a béke és a biztonság pedig sérülékennyé válik. Jövőnk veszélyeztetettebb lesz, kevésbé jól tervezhető és előre látható. A korábbi stratégiai egyensúly felbomlik. Végeredményképpen a digitalizáció alapvetően megváltoztatja a biztonsági helyzetet. A világpolitikai zűrzavar ősrövese fenyeget, és pedig az utolsó nagy ipari forradalom óta a történelemben nem is először.

Nélkülünk: a helyettesítő keresése

„A 21. században megszületett a helyettes háború koncepciója.”^[46] Jean-Marc Rickli a Harvard Kennedy Schoolon működő Future Society agytröszt mesterségesintelligencia-iniciatívájának főtanácsadója, valamint a letális autonóm fegyverrendszerek szakértője az ENSZ-nél. A genfi Biztonságpolitikai Központban az új biztonságpolitikai kihívások kérdéseivel foglalkozik. A helyettes háborúk esetén szerinte a konfliktus résztvevői olyan helyettesítőket keresnek, amelyekkel dűlőre vihetik konfliktusaikat és háborúskodásaikat. Emberek vagy gépek szolgálhatnak ilyen pótlékként.

A nagyhatalmak már a 20. században is vívtak helyettes háborúkat, hogy elkerüljék a közvetlen katonai konfrontációt. A digitális 21. században keressük azt az új fogalmat, amely képes kifejezni a digitális háborúpótlék dimenzióit. „Helyettes háború”: így hangzik az új, politikai kifejezés, amely olyan konfliktus-

tust jelöl, mely immár nem a clausewitzi hármasságeszmét aktualizálja, s ezért nem egykönnyen ismerhető fel háborúként. A demokratikus vagy autokratikus államok ugyanis ahelyett, hogy a biztonság megőrzése vagy megteremtése érdekében nemzeti fegyveres erőiket vetnék be, pótlékot keresnek a helyükbe, s erre a helyettesítőre – a katonai szolgáltatókra – már a múlt évszázad kilencvenes éveiben rátaláltak. Magántulajdonban lévő katonai vállalkozókról és hadiipari cégekről van szó, amelyek ajánlatok sokaságát kínálják a kormányoknak a logisztikától a zsoldos-szolgáltatásokig, hogy háborús cselekmények során vagy válságövezetekben támogatást nyújtsanak. Közülük számosan nagy súlyt helyeznek arra, hogy csak a nemzetközi jog által elismert olyan alanyok szolgálatába lépjenek, amelyek tiszteletben tartják az emberi jogokat és a humanitárius nemzetközi jogot.^[47]

A Blackwater cég, amely egy cégfelvásárlás nyomán ma Academi márkanéven tevékenykedik, éppúgy a katonai vállalkozások közé tartozik, mint az ártatlan nevet viselő Computer Science Corporation (CSC) vagy a legmodernebb harceszközök előállítói – a Krauss Maffeitől a Thalesig. Az amerikaiak által az iraki háborúban bevetett Predator drónokat a gyártó civil munkatársai működtették.^[48] Németországban a Rheinmetall hadiipari konszern üzemelteti a Bundeswehr legnagyobb csapatgyakorlótérét, a „Gefechtsübungscenter Heer”-t.

Nem vehetjük kritika nélkül tudomásul, ha kormányok demokratikus választások útján rájuk ruházott, a köz biztonságának megőrzésével kapcsolatos feladatokat nem állami vállalko-

zásokhoz szervezik ki. A biztonság ugyanis ilyenkor nem csak hogy a forgalom és a nyereség tárgyává válik, amit a piac szabályai szerint a legjutányosabb áron kínálnak, hanem másodlagos fontosságú is lehet, hiszen üzletet csak a háború tesz lehetővé, a béke nem. Azok a kormányok, amelyek a biztonság ügyét nem állami szereplőkre ruházzák át – mert saját hadseregekre vagy biztonsági kísérő egységeikre nem támaszkodhatnak –, ráadásul magukat gyengítik, ha helyettesítő embereiknek náluk eredményesebben sikerül gondoskodni arról, hogy a népesség mindennapi élete biztonságos, vagy legalább előrelátható legyen.

A legrosszabb esetben a nem állami csoportok a biztonság megteremtése során önállósíthatják magukat, olyan saját normatív rendszereket hozva létre, amelyek a háborús területeken garantálják a lakosság számára a közeli jövő bizonyos mértékű kiszámíthatóságát („Vajon holnap is mehetünk dolgozni?”). Erőszakosan és szörnyű eszközökkel, de saját magatartási szabályaik megalkotásával még a tálibok és az Iszlám Állam is verseng a megfelelő államok törvényes kormányaival a hatalomért. (Vagyis, ami az utóbbit illeti: *versengett*, amíg még volt földrajzi terület, amelyre és amelynek lakosságára a fennhatósága kiterjedt.) Ezért aztán egy állam, amely privatizálja a biztonságot, tartósan csak akkor várhatja el, hogy respektálják, ha fenn tudja tartani fölényét helyettesítőivel szemben. Ehhez képesnek kell lennie arra, hogy állami kényszert alkalmazva, szociális kapcsolatait megrendszabályozva és népességét meggyőzve felülkerekedjen a magánkonkurencián. ^{[49], [50]}

A közbiztonság gazdasági alapokra helyezésében azonban bizonyos mértékig a népesség sem érintetlen. Noha változatlanul elvárja a biztonságot, mint közjót, kormányai számára azonban egyre inkább megnehezíti, hogy azok gondoskodjanak is róla. „Manapság azt tapasztaljuk, hogy a clausewitzi hármasság egy olyan dinamika hatása alá kerül, aminek során az emberek kikerülnek az egyenletből, és különböző okokból valami más helyettesíti őket. Ennek legnyilvánvalóbb oka, hogy az erőszak alkalmazása, mindenekelőtt a demokráciákban, egyre nehezebben képviselhető, a kormányt viszont felelőssé teszik érte, különösen csapatok külföldre küldése esetén. Aki helyettesítőt talál erre, csökkenti a saját kockázatát”, vonja le a végkövetkeztetést Jean-Marc Rickli.^[51]

Noha a társadalom az Európai Unióban is ismét növekvő készséget mutat arra, hogy maga szálljon síkra rendszere védelmében, „azon a ponton mindig saját korlátaiba ütközik, ahol a klasszikus hősiességre van szükség”,^[52] foglalja össze a helyzetet Wolfgang Ischinger, s ezt úgy érti, hogy nincsenek hősök, akik készek lennének „életük kockáztatásával kiállni egy olyan közügyért, amiben hisznek”.^[53] A népesség nem fogadja el, hogy a biztonságért nagy áldozatokra lehet szükség. Ezért is jön épp kapóra a digitális haladás, az egymást sűrűn követő fejlesztések a robotika és a mesterséges intelligencia területén. Úgy tűnik, mintha az intelligens gépek azt ígérnék, hogy az emberek a háborúban is helyettesíthetők lesznek. A terroristák ellen földi csapatok helyett biztos távolságból vezérelt drónokat vetnek majd be. Azok a gépek, amelyek a jövőben a repülőalakzatok

szélén haladva védik az ellenséges légitámadások ellen a légteret a pilóták vezette harci gépekkel együtt, vezető nélküli harci drónok lesznek. Egyáltalán: a „cybertér”, ami az államokat, nem állami szereplőket és (intelligens) gépeket egyetlen új ökoszisztémába vonja össze, nem más, mint maga a háború pótléka.

A környezeti intelligencia mint csatatér

Mindennapjaink tárgyai mintegy varázsütésre életre kelnek, és kognitív képességeket mutatnak. Mesterséges intelligenciával feltöltve hálózatokba lépnek az emberekkel, de más dolgokkal is, és információkat cserélnek vagy stimulusokat küldenek egymásnak. Egyre több szereplő van fenn a neten és vesz részt a mindennapi életben, szünet nélkül interakciókat folytatva és kommunikálva. Ez zajlik a *minden internetjén*, amelyhez rendszerreleváns infrastruktúrák szenzorai – például elektromos és közlekedési hálózatokéi, ipari létesítményekéi és járművekéi – vagy emberek csatlakoznak, utóbbiak okostelefonok, okosórák és bőrükre rögzített vagy bőrük alá implantált chipek révén. Környezetükből származó mérési adatokat regisztrálnak, és drótnélküli összeköttetés útján továbbítják őket egy reléállomásnak vagy egy számítógépes felhőbe, ahol más gépek – köztük számtalan olyan, amelyben mesterséges intelligenciát alkalmaznak – elemzik őket, mielőtt tényezőkké lennének az optimalizálandó környezeti ingerek kiszámítása során.

A metafora, amivel a jogtudományi kutatás az általános hálózatiságot és ennek (hálózatba kapcsolt) hétköznapi objektu-

mok révén adódó kognitív potenciálját megnevezi, az *ambient intelligence*,^[54] a környezeti intelligencia. Az emberek, a gondolataik, a szándékaik, a pszichéik és tárgyaik hálózata ily módon napról napra értékesebb lesz, a hálózat növekedésével pedig egyre kívánatosabbnak tűnik a környezeti intelligencia politikai és katonai célú felhasználása a geopolitika eszközeként. E jövőbeli csatatéren – a szereplők szándékai szerint – a cél az irányítás átvétele vagy már létező államhatalmak és társadalmi struktúrák további fenntartása, a demokráciáé éppúgy, mint a diktatúráé.

A társadalom közösségi megakomputerré való átalakítása, úgy tűnik, lehetővé teszi, hogy lemondjunk a klasszikus katonai eszközökről, és mégis folytassunk háborúkat. A digitalizáció a hatalom és az erőszak újfajta eszközeit teszi lehetővé. A digitális kémkedés, szabotázs és online szubverzió azok a műveletek, amelyek a 21. században a katonai erő bevetésének alternatíváiként szolgálnak. Online akciókkal is elő lehet ugyanis idézni a környezeti intelligencia súlyos károsodásait, ami a legrosszabb esetben emberéleteket is követelhet, véli John Brennan, aki 2017-ig állt a CIA élén:

„Önök a cybertérben olyan dolgokat tehetnek, amelyek alatomosabbak, talán némiképp kifinomultabbak, de éppoly hatásosak [mint a katonai erőszak fizikai alkalmazása], mert más országok infrastruktúráját és képességeit béníthatják meg velük.”^[55]

Ugyanakkor nem újdonság a nem katonai eszközök felhasználása politikai célok elérése érdekében. Ha technikailag meg

lehetett valósítani őket, úgynevezett nemlineáris, hibrid intézkedések formájában gyakran a múltban is katonai műveletek velejárói voltak. Az új évezred környezeti intelligenciájában azonban járulékos katonai akciók nélkül alkalmazhatók. Ennek során a támadókat védi a környezeti intelligencia megosztott és anonim struktúrája, mert csak nehezen lehet megállapítani, hogy valójában ki is volt egy támadás elindítója.

„Nézzük csak meg, hogyan alkalmaz erőszakot a cybertérben az orosz kormány... Trollgyárakat tart fenn, és olyan narratívákat hint el a világban, amelyek hólabdahatást indítanak be. Aztán ott van az a hihetetlen gyűlölet, ami kész kitörni. Az orosz kormány nagyon jól megértette ezt a dinamikát, és dezinformációs kampányok, lélektani hadműveletek során hasznosítja.”^[56] Jean-Marc Rickli szóhasználatával ez erőszak-alkalmazás, csak tipikus katonai eszközök nélkül.

Hibrid hadijátékok

Az államok nem csak katonai vállalkozásokra támaszkodnak, ha ki akarják szervezni háborúikat. Azok körébe, akiket egy kormány igénybe vehet, beletartoznak bűnözők, hekkerek, kémek, újságírók is, továbbá mindazok, akik be akarják hízelegni magukat a kormányuknál. A digitális korszakban kamatoztatják képességeiket, legyen szó akár információk gyűjtéséről, propaganda internetes terjesztéséről, adatlopásról, vagy *ransomware*, zsarolóprogram segítségével elkövetett zsarolásról.

A magánszektor ebben a vonatkozásban tekintélyes képességekkel rendelkezik, amelyeket egyaránt kihasználnak az amerikai, orosz és kínai titkosszolgálatok, hogy digitális műveleti képességeiket hosszú távra kialakítsák.^[57] És ehhez még csak sok pénzre sincs szükség! Azért az összegért, amit az Egyesült Államok egyetlenegy F-35-ös sugárhajtású harci gépért kiad – a kiviteltől függően nagyjából 100 millió amerikai dollárt –, Moszkva be tud rendezni egy olyan irányítóközpontot, amely maradéktalanul integrálja Oroszország elektronikus hadviselési, online propaganda- és hekkerpotenciálját. A környezeti intelligencia elleni támadások ugyanis sokkal olcsóbbak egy katonai csapásnál. Ugyanakkor egy olyan, környezeti intelligencia elleni, jól megtervezett, összehangolt támadás hatása, amelynek súlyossága még éppen egy katonai csapás szintje alatt marad, a lakosság szempontjából pusztítóbb lehet, mint a legújabb generációhoz tartozó harci gép legmodernebb precíziós fegyvereinek bevetése, amely a sebészi pontosságú gyilkolás lehetőségével kecsegtet. Vagy másként megfogalmazva, egy digitális hadművelethez nem kell sok, hogy teljes katasztrófát idézzon elő.^[58]

„Ezen a ponton – mutat rá Jean-Marc Rickli – a helyettes háború átalakul hibrid folyamattá, mert a szereplők elkezdenek a hadviselés számos különböző szintjével játszani”, majd azzal fejezi be, hogy ebben semmi új nincsen. Az ellenfél bomlasztása, demoralizálása vagy diszkreditálása mindig is a katonai erőszak kísérő jelensége volt. Egy olyan politika számára azonban, amely politikai céljainak elérése érdekében az ilyen intézkedéseket a katonai erőszak klasszikus kellékei nélkül alkalmazza, a

hibrid támadások a politika eszközeivé lesznek. Aki a háborút így értelmezi, újradefiniálja annak jelentését. A hibriditás lehetővé teszi a nem sokkal a hadüzenet-küszöb alatti hadviselést. Így a háború és a politika többé nem *vagy-vagy*: a háborúnak – Clausewitz korával ellentétben – többé nem az a célja, hogy egy pontosan meghatározott ellenfelet egy pontosan meghatározott időpontban egyértelműen legyőzzenek; immár elmosódottá válik, hogy egy háború mikor kezdődik, hogy egyáltalán fennáll-e (már) a háborús állapot, hogy ki vívja a háborút, és hogy meddig fog tartani. A hibriditás korában a clausewitzi világ elavul, és többé nem nyújt megfelelő értelmezési keretet a háborúhoz. A háború és a béke közötti határok elmosódnak, a konfliktusok pedig lefojtva parázsló, nyílt végű ellenségeskedések lesznek, miközben nem egyértelmű, ki az ellenség, hol húzódnak a határok, és hogy valójában kik a hadviselő felek.

Csak mert egy hibrid jellegű háborúhoz nem tartozik hozzá a katonai erő alkalmazása, a biztonsági szakemberek már nem háborúról beszélnek: „fenyegetéssé” fokozzák le a hibrid intézkedéseket. A hibrid fenyegetés magának a háborúnak immár alternatívája, helyettesítője lett, állandó pozícióra tesz szert a politikában, és amolyan „gerilla-geopolitikaként” a megtámadott gyengéit veszi célba,^[59] aminek során azonban kerül a nyílt katonai cselekményeket. Ha így nézzük, lehetséges, hogy a NATO nem a megfelelő háborúra készül fel, amikor katonai szövetségként több alakulatot állomásoztat keleti határain, vagy nukleáris arzenáljának újabb bővítésétől remél előnyöket, ahogyan azt

Donald Trump, az Egyesült Államok 46. elnöke 2018-as nemzetvédelmi stratégiájában lefektette.

Választási titkok

2016 júniusa van, keddi nap, amikor az amerikai elnökválasztás kaliforniai előválasztásait tartják Riverside megyében. Az önmagát kívülállóként meghatározó Donald Trump a washingtoni hatalmi apparátust hívta ki Hillary Clinton személyében.

A szavazóhelyiségek megnyitása óta Michael Hestrin kerületi államügyész irodájában egy pillanatra sem hallgatnak el a telefonok, panasz panaszt követ. A választásra jogosultak hiába próbálják meg leadni szavazatukat.^[60] Felvetődik az online manipuláció gyanúja. A párthovatartozáshoz szükséges előzetes regisztrációt a kaliforniai választásra jogosultak tudomása nélkül, de egyértelműen a személyes adataik – többek közt a társadalombiztosítási számuk és a jogosítványszámuk – felhasználásával valakik megváltoztatták.^[61]

Mivel a választás szervezői által a szavazásban akadályoztatott polgárok formális panaszai egyre sokasodnak – Mike Hestrin heves szóváltásokról számol be, amelyek a választók, a választás szervezői és megfigyelő közt zajlanak –,^[62] a kerületi ügyész nyomozókat küld a választóhelyiségekbe, hogy előzetes vizsgálatot végezzenek. A kaliforniai választási rendszer amúgy is kritika tárgya. Miközben a *Grand Old Party*, a GOP – ahogyan a republikánusok más néven hívják magukat – republikánus

választóinak mindig regisztrálniuk kell a választások előtt, a *Sunshine State* nem regisztrált demokratáknak is megengedi, hogy az előválasztásokon szavazólapot adjanak le. Mindazonáltal csak ideiglenest, és a formátuma is különbözik a már regisztrált demokratákéitól. Ha hiányzik a speciális, átjelentkezést bizonyító szavazólap, a szavazatot annullálják.^[63]

Amit a nyomozók a helyszínen, a választóhelyiségekben megállapítanak, első ránézésre mégis megnyugtatónak tűnik. Azok a választók, akiknek a regisztrációjával valami nincs rendben, ideiglenesen azért szavazhatnak. Az ideiglenesen leadott szavazatok összeszámlálása mindazonáltal több időt vesz igénybe, mert előzőleg még ellenőrizni kell az egyes szavazók választási jogosultságát, hogy szavazatuk végül is számítson. Ezért aztán nem egy szavazó mindjárt teljesen lemond voksa leadásáról.

Amikor a szabálytalanságokról kérdezik, a kaliforniai *secretary of state*, a demokratikus eljárás őrének számító Alex Padilla szóvivője megnyugtatóan közli: „Választópolgárok milliói regisztráltatták magukat interneten és papíron, de csak csekély számú panasz érkezett hozzánk ebben a választási ciklusban. (...) A problémák a legtöbb esetben véletlen tévedésekből származnak. A választók, amikor frissíteni akarják regisztrációjukat, néha hibáznak, és egyszerűen megfélekednek regisztrált párttagságukról, vagy nem találják meg a nevüket szavazóhelyiségük szavazói listáin.”^[64] Ez egyébként ugyanaz a reakció, mint amit a Microsoft a WannaCry zsarolószoftver felbukkaná-

sának napján produkált, tudniillik, hogy maga a számítógép-felhasználó a hibás. Ezúttal a szavazó a hunyó.

Ugyanekkor Washingtonban John Brennan, aki 2017-ig töltötte be a CIA igazgatói tisztét, felettébb riasztónak találja a fejleményeket. Ő ugyanis több információval rendelkezik, mint a kaliforniai, helyi politikusok, a választók és a szervezők – ráadásul más jellegűekkel. A CIA figyelte az oroszok amerikaiak elleni cybertámadására, amely agresszivitás és intenzitás tekintetében mindent felülmúlt, amit eddig a régi ellenségtől a szovjet időkből szokványos politikai beavatkozásaként megszoktak.^[65] „[Az oroszok] feltérképezték az [amerikai] választási infrastruktúrát, és megfigyelték az állami rendszereket.”^[66]

Az amerikaiak jól tudják, hogy az oroszok miként készítenek elő katonai műveleteket. A támadás előtt felderítik a célpont környezetét, hogy pontosabban megértsék, hol kell támadniuk, és milyen előnyre tehetnek szert egy támadással. Az eljárást *operational preparation of the environment*nek, a környezet műveleti előkészítésének nevezik.

A CIA számára 2016 nyarán teljesen nyilvánvaló, hogy a hidegháborús időkből ismert régi ellenfél az amerikai választási rendszereket vette célba. Az online behatolás arra enged következtetni, hogy Oroszország olyan támadásra készül, amely meglepi majd ez Egyesült Államokat. Miközben a kaliforniai miniszter, Alex Padilla még a felborzolt választói kedélyeket igyekszik megnyugtatóan anélkül, hogy tudná, mi zajlik valójában, a két nagyhatalom között már teljes erővel tombol a vihar – mindenestre John Brennannek ez a kellemetlen benyomása támad. Va-

lamit tennie kell, ezért először az FBI-t tájékoztatja, hogy a szövetségi hatóság intézkedéseket léptethessen életbe a választási infrastruktúra védelmére.

Időközben Mike Hestrin nyomozóinak is feltűnt, hogy a kaliforniai választási rendszer hekkertámadások következtében meghibásodott. Emellett szól az is, hogy a két párt, mind a demokraták, mind a republikánusok, az előválasztások napján egyaránt döbbenten tapasztalták, hogy a választói regisztrációval gondok vannak. Hestrin azonban nem tudja visszakövetni a támadásokat a támadókhoz. A digitális kaliforniai választási rendszer nem jegyezte fel a hekkerek IP-címeit, így a tettesek nyomai a semmibe vesznek, zsákutcába vezetnek.

A magyarázat végül Illinois államból érkezik, ahonnan néhány héttel a kaliforniai incidens előtt jelentették, hogy 109 választási rendszerét malware-ekkel fertőzték meg, amelyek lehetővé tették a hozzáférést az aktuális és korábbi választások 15 millió választójának fájljaihoz. A választási rendszerbe behatolóknak a szavazók listáin szereplő neveket és címeket sikerült megváltoztatni – sőt még törölni is. Hasonló feltűnő eseményeket jelentenek most már más szövetségi államokból, Tennesseeből, Új-Mexikóból és Floridából is. Végül az amerikai szövetségi államoknak több mint a fele érintett.

Illinois azonban nemcsak biztonsági másolatot készített választói jegyzékeiről, hanem ezúttal a tetteseket is sikerül kinyomoznia. Digitális ujjlenyomatuk és hekkelési módszerük alapján a nyomozók az APT28 néven is tevékenykedő, orosz Fancy Bear hekkerközösséghez tudják kapcsolni a támadást. Igaz,

hogy a hekkerekről senki sem tud közelebbit, egy dolog azonban biztos: hogy a Fancy Beart az orosz állami titkosszolgálat irányítja.

Az orosz hekkelés belpolitikai következményei meglepők, mindenekelőtt azonban meglepően sikeres orosz szempontból: működni kezd a bomlasztás. A republikánusok és a demokraták kölcsönösen egymást gyanúsítják a választásokba való beavatkozással.^[67] És a java még hátra van: kevéssel azután, hogy fény derült a választási rendszer megrongálásának első néhány esetére, a republikánusok elnökjelöltje, Donald Trump kizárja annak lehetőségét, hogy Moszkva beavatkozott az amerikai elnökválasztásokba, s ehelyett a demokratákat vádolja meg önmaguk a célból való meghekkelésével, hogy eltereljék a figyelmet az elnökjelöltjükkel, Hillary Clintonnal kapcsolatos számos problémáról.^[68]

Washingtonban még kétségesnek tűnik, hogy vajon az előválasztások idején végrehajtott orosz hekkertámadás nem csak annak a próbája volt-e, hogy a tulajdonképpeni választási napon, 2016. november 8-án maximális káoszt idézzenek elő – ahogyan azt sem tudják, hogy az oroszok valójában milyen súlyos károkat tudnának okozni. Elképzelhető volna, hogy az orosz kormány távirányítással úgy tudja befolyásolni az amerikai elnökválasztást, hogy az általuk óhajtott jelölt, Donald Trump kerekedjen felül? Mindenesetre abból kell kiindulni, hogy csak a gyengébb támadásokat fedezték fel. Kína mellett mégiscsak Oroszország rendelkezik a világ legprofesszionistább és leggyorsabb hekkereivel. Tizenkilenc perc: ennyi ideje van

egy-egy áldozatnak, mielőtt egy orosz támadás megfertőzi, kifosztja vagy lezárja a hálózatát.^[69] A csakugyan sikeres támadások – a szövetségi hatóságok kénytelenek ezt feltételezni – alighanem még csak fel sem tűntek senkinek.

Csak egyvalami volt világos: az orosz hekkerek nem egyszerűen azért loptak információkat a választási rendszerek adatbankjaiból, hogy titkosszolgálati használatra felderítést végezzenek. Itt sokkal többről és egészen másról volt szó, mint információszerzésről: neveket kellett eltüntetni vagy lecserélni, hogy ezzel akadályozzák az amerikai választópolgárokat szavazataik leadásában, vagy megghiúsítsák a szavazatszámlálás eredményeinek későbbi továbbítását.

Közben bekapcsolódott a vizsgálatba a Jeh Johnson belbiztonsági miniszter vezetése alatt álló Department of Homeland Security is. Johnson telefonkagylót ragadott, és sorra hívta a szövetségi államokat, hogy felajánlja segítségét a választási intézmények védelméhez, valamint a sebezhető pontok felderítéséhez. A szövetségi államok reakciója azonban mereven elutasító, sőt felháborodott. „Gondoskodjon róla, hogy a washingtoni kormány távol tartsa magát az államunkban jelentkező választási problémáktól”, hangzik az illetékes hivatalnokok ingerült válasza.^[70] Bizalmatlanok. Attól tartanak, Washington esetleg megpróbál beavatkozni a szövetségi ügyeikbe. Különösen Johnsonnak az a javaslata bizonyul kevésbé hasznosnak, hogy nyilvánítsák a kritikus fontosságú infrastruktúra részének a választási rendszereket, ezzel tegyék egyenrangúvá az energia-, a közlekedési, vagy a banki hálózattal.^[71] A kritikus infrastruktúrák-

kal kapcsolatban ugyanis különleges biztonsági követelményeket érvényesítenek, ilyen alapon tehát a washingtoni kormány hozzáférhetne a helyi választók adataihoz, és rendszeresen kommunikálhatna a választási szisztémát helyben működtető tisztviselőkkel.

A növekvő bizalmatlanság légkörében az amerikai szövetségi államok és hatóságai körében ekkor az a gyanú kap lábra, hogy Washington maga avatkozik be az amerikai választási rendszerekbe és sérti meg integritásukat,^[72] hogy afféle partizánháború során fejtsen ki ellenállást a republikánus elnökjelölttel, Donald Trumppal szemben. Utóbbi pedig, ahelyett, hogy indítványozná egy külhatalom nyilvánvalóan ellenséges szándékú támadásának felderítését, a két elnökjelölt második televíziós vitája során e kijelentésre ragadtatja magát: „Talán nem is volt hekkertámadás.”

Ez belpolitikai megközelítésben: katasztrófa – s már csak ezért is jól érzékelteti a kívülről végrehajtott digitális támadás előnyeit. Az ilyet egész egyszerűen nem veszik komolyan – vagy gyorsan kétségbe vonják, hogy megtörtént. Bárki elindíthatta ugyanis az attakot akár az ellenfél választási küzdelmét szervező team is – belföldről. Annak végül is minden oka megvan rá, hogy a személyt, aki egy rövid időre a másik politikai tábor exponense, minden eszközzel hátráltassa, immár nemcsak politikai eszközökkel, hanem megkérdőjelezhető és illegális digitális befolyás érvényesítésével fizikailag és lélektanilag is... Ily módon addig áthághatatlan határt léptek volna át.

Ugyanekkor Washingtonban John Brennan egy másik megkerülhetetlen kérdéssel szembesül: vajon az orosz kormány, vajon személyesen Vlagyimir Putyin politikai beavatkozást rendelt el a 2018. november 8-iki amerikai választásokba, és a választás napjára tervez valamit a választók ellen vagy a szavazatszámlálás megzavarására? „Ez számomra [mondta John Brennan] egyet jelentene a háborúval.”^[73]

Az attribúció kérdése – tehát hogy egy államnak egy másik ellen elkövetett erőszakos támadását egyértelműen hozzárendeljük valakihez – jogilag és katonailag egyaránt lényeges, hiszen azonnal felvetődik a kérdés, milyen védelmi és megtorló intézkedések vethetők be. Ugyanis: még a háború sem jogilag szabályozatlan szféra.

E forgatókönyvön belül a védekezésnek három esete képzelhető el:

Először is: közvetlen kapcsolatba lehet lépni az oroszokkal, és óva inteni őket attól, hogy beavatkozzanak az Egyesült Államok politikai ügyeibe.

Erre maga John Brennan tett kísérletet, amikor 2016. augusztus 4-én felhívta Alekszandr Bortnyikovot, az orosz titkosszolgálat, az FSzB vezetőjét.^[74] A közvetlen telefonkapcsolat azért állt fenn Oroszországgal, mert a két állam rendszeresen véleményt cserélt a szíriai helyzetről.^[75] Mindenesetre Bortnyikov a várakozásoknak megfelelően reagált, kereken visszautasította, hogy beavatkoztak volna az amerikai belpolitikába.^[76] Az ügy pedig eszkalálódott. A 2016. szeptemberi hangcsoui G20-as csúcson

Barack Obama félrevonta Vlagyimir Putyint, és lelkére kötötte, hogy őrizkedjék „a vadnyugati stílusú hekker-háborúktól”.^[77]

Másodszor: mennyi információt szabad kiadni az amerikai lakosságnak?

A hírszerzési tevékenységgel kapcsolatban mindenkor felvetődik a titokvédelem kérdése. Brennan csak annyi információt fedhetett fel, amennyivel sem forrásaira nem utalt, sem módszereit nem árulta el. Ennek érdekében Washington egy gondosan megfogalmazott sajtóközleményt készített elő, amely azonban semmiféle következtetésre nem adott módot Putyin felelősségére a szövetségi államok elleni támadásokat illetően^[78] – jól lehet minden arra utalt, hogy személyesen Putyin adott parancsot rájuk.^[79] Úgy döntöttek, a közleményt 2016. október 7-én, helyi idő szerint 15 óra 30 perckor adják ki. Rendes körülmények között egy péntek délutánt taktikailag okosan megválasztott időpontnak tarthatnánk: nem sokkal ezután zárnak a tőzsdék – a kellemetlen gazdasági híreket az emberek a hét végén megemésztették volna. Kezdődött a hétvége, és Washingtonban úgy vélték, kinek-kinek lesz majd ideje, hogy reflektáljon egy ilyen horderejű politikai hírre, hogy megvitassák, és hogy kellő komolyságot tulajdonítsanak Oroszország beavatkozásának. Csakhogy másként történt.

Alig fél órával azután, hogy megjelent a tévéképernyőn az amerikai kormánynak az elnökválasztásokba való orosz beavatkozásra vonatkozó közleménye, és kevéssel egymás után mindjárt két bomba is robban a médiában. Helyi idő szerint 16:03-kor a *Washington Post* közzétett egy videót, amelyben Donald

Trump saját, hollywoodi hírességeknél alkalmazott csábítási kunsztjaival hencegett: *Grab them by the pussy*, „alá kell nyúlni nekik”.

A video *Donald Trump Access Hollywood Tape*, avagy *Pussygate* néven került be a hírességek számos szexbotrányának történetébe. A felvétel egyértelműen káros lehetett volna a republikánusok számára, és jócskán árthatott volna esélyeiknek a választás kedvező kimenetele szempontjából. Árthatott volna – de nem ártott. Amerikának ugyanis mindössze 29 perce volt a felhördülésre, hogy spekulálni kezdjen elnökjelöltjének hollywoodi szexügyeiről, és már fel is gördült az amerikai választási krimi következő felvonásának függőnye. A második felvonás aztán jóval hosszabban fejtette ki hatását, és nem ment oly gyorsan feledésbe, mert James Comey, a Donald Trump által 2017-ben leváltott FBI-igazgató, még röviddel a 2016. október 8-iki választás előtt büntetőjogi vizsgálat tárgyává tette.

16:32-kor a WikiLeaks apránként megkezdi Hillary Clinton e-mailjeinek a nyilvánosságra hozatalát, amelyeket néhány héttel korábban loptak el tőle. Jóllehet a *Pussygate* rossz fényt vet Donald Trumpra, a demokrata táborból származó, kerek fél évvel korábban hekkerek által megszerzett e-mailek ismertté válása el tudja terelni a figyelmet Donald Trump nőellenes alapállásáról.

Vajon lehet-e véletlen a történetek időbeli egymásutánja? Az orosz beavatkozással kapcsolatos washingtoni kormánynyilatkozat olyan rövid életű volt, hogy azt senki sem sejthette előre. Közzététele után mindössze 32 perc alatt a történelem lábjegy-

zetévé jelentéktelenült. Az oroszok amerikai belügyekbe való beavatkozásának jelentősége másodrendűvé vált. Egyszerre ugyanis, felettébb dicstelen módon, Donald Trump lett a közbeszéd tárgya, de ő sem sokkal tovább, mint maga a kormánynyilatkozat, mert a WikiLeaks publikációi már ismét neki kedveztek.

Az Obama-kormányzatnak keservesen meg kellett tanulnia, hogy a stratégiai kommunikáció komoly kihívás az online agresszió korában, és minden átmenet nélkül kommunikációs katasztrófába torkollhat.

Harmadszor, és ez az utolsó elképzelhető védelmi opció: Mi a helyzet egy ellentámadással?

John Brennan nagyon komolyan mérlegeli a kérdést, ám elsősorban Barack Obama az, aki visszaretten attól, hogy óvatos intézkedéseknél messzebb mutató lépéseket tegyen az orosz beavatkozás ellen. A Fehér Ház nem akarja kockáztatni egy hekerháború eszkalációját Oroszországgal, és annak sem óhajtja kitenni magát, hogy az elnökválasztásba való beavatkozás vádja még hangosabbá váljon. Semmiképp sem keletkezhet az a látzat, hogy egy demokrata kormányzat támogatja ugyanezen párt elnökjelöltjét, Hillary Clintont. Így hát a Fehér Ház cyberelhárításának meg van kötve a keze, és vészhelyzeti tervről egyeznek meg a 2016. november 8-iki választás körüli napokra.

„Amennyiben »jelentős cyberincidens« következne be, amely »igazolhatóan befolyást gyakorol a választási infrastruktúrára«, »a belbiztonsági hatóságok, az FBI és a nemzeti hírszerző szol-

gálatok igazgatói« továbbfejlesztett eljárásokat aktiválnak, illetve erőforrásokat helyeznek készenlétbe.”^[80]

A nemzeti erőforrásokra való utalás főképpen katonai lépést jelent: a védelmi minisztérium „egy szövetségi hatóság és a védelmi miniszter, vagy az elnök ajánlására támogatást nyújthat a polgári hatóságoknak a cyberincidensekre való reagálás során”.

^[81] Vajon ez annyit tesz, hogy a fegyveres erők a választóhelyiségek előtt járőröznek majd? „A rendelkezésre álló nemzeti erők lehetnek tartalékosok, a fegyveres erők aktív tagjai és a Nemzeti Gárda.”^[82]

Ez úgy hangzik, mint egy részleges mozgósítás. Az elgondolás nyilvánvalóan az, hogy aktivizálják a védelmi minisztérium cyberelhárítási kapacitását.^[83] Noha a törvény alapvetően tiltja, hogy az amerikai kormány fegyveres erőt alkalmazzon a nyitva tartó választóhelyiségekben vagy azok előtt, az igazságügyi minisztérium az említett vészhelyzeti tervvel kapcsolatban kiáll amellett, hogy nagyon is szabad katonai erőt bevetni, ha egy választóhelyiséget egy cybertámadás teljesen megbénít és nem lehet további szavazatokat leadni.^[84] Alkalmazható tehát olyan válság-forgatókönyv, mint természeti katasztrófák esetén, amihez egyfelől stratégiai kommunikáció társul a választás szabályossága iránti bizalom fenntartása érdekében, másfelől három napos cybervédelmi riadókészültség a választás tulajdonképpen időtartamán túl.

A tervet a Fehér Ház végül soha nem hagyja jóvá.^[85] A választás napján az orosz beavatkozások egyébként is csak az előválasztások idején tapasztalt szinten mozognak. A szavazat-

számlálás során ezzel együtt az egész világ visszafojtja lélegzetét.

Minden prognózis dacára a republikánus tábor egymás után szerzi meg az egyes államokat. Óráról órára csökken a mérsékelt politikai stílus reménye. A meglepetés még a választás éjszakáján teljessé válik: Hillary Clinton nem lesz az Egyesült Államok első női elnöke. A *president elect* Donald Trump: az Egyesült Államok 45. elnökének hivatalát a manhattani ingatlanfejlesztő tölti be.

Bizonyítékok hiányában

A hibrid támadások kiszervezése a megtámadott államot nagyon súlyosan érintheti, ugyanakkor jelentősen megnehezíti a hibrid támadás attribúcióját – valamely államhoz kötését. A megtámadott sohasem lehet biztos abban, hogy hibrid állami támadásról, vagy pedig magánemberek magánérdekből elkövetett bűncselekményéről van-e szó. Mutasson bár minden jel egy hibrid állami támadásra, valamennyi bizonytalanság mindig marad. Egyáltalán be tudná bizonyítani egy megtámadott állam, hogy egy másik állam volt az, amely a hibrid támadást kitervelte, és helyettesítő segítségével kivitelezte? Másként fogalmazva: mennyire lehetett biztos abban az Egyesült Államok, hogy a Kreml beleavatkozott az amerikai választásokba? Vajon az államok közössége, sőt, az állam saját népessége meggyőződhet-e volna, hogy egy idegen államtól kiinduló támadásról van szó, amit el kell ítélni, illetve szankcionálni kell? A hibrid fenyegetés lé-

nyegéhez ugyanis kifejezetten hozzátartozik, hogy az áldozatot megakadályozzák abban, hogy védekezzen és katonai ellencsapást hajtson végre.^[86] Ez finom érzéket igényel a támadó részéről: azt kell mérlegelnie, mekkora eszkalációt engedhet meg magának, hogy még az államközi háború küszöbe alatt maradjon. Ez is része az újfajta hatalmi berendezkedésnek: mármint annak demonstrálása, hogy egy állam elégséges hatalommal rendelkezik a kényszer mértékének fokozására.

Egyes szakértők már abból indulnak ki, hogy egy hibrid támadás forrása manapság 80 százalékos bizonyossággal beazonosítható.^[87] Egyvalamivel azonban tisztában kell lennünk: miközben az államok többsége továbbra is sötétben tapogatózik, az amerikaiak egyre sikeresebbek a visszakövetésben. E célból a Nemzetbiztonsági Ügynökség, az NSA érzékelőeszközöket telepít világszerte, amelyek mindent, ami a környéki intelligenciában történik, radarrendszerhez hasonlóan ellenőriz. Ezért aki tudni akarja, hogy hibrid támadás áldozatává vált-e, és hogy ezt ki követte el, ha jó és kellően bizalmas viszonyban van az Egyesült Államokkal, kérheti, hogy tájékoztassák – persze nem ingyen: mindig a nézőponttól függően magas árért, információcsere fejében, vagy még nagyobb megfigyelés fejében.^[88]

A kérdés, hogy egyáltalán hibrid támadásra kerül-e sor, illetve hogy ki az elkövetője, központi jelentőségű a nemzetközi jog, a *ius ad bellum* alkalmazhatósága szempontjából, ami szabályozza, hogy a háború viselésének joga alkalmazható-e, s ha igen, miképpen. Az államok közössége egyelőre még nem ismer egyezményes és kötelező standardokat, amelyek meghatároz-

nák, hogy egy hibrid támadás meddig pusztán fenyegetés, és mikortól háborús cselekmény. A kérdés igencsak időszerű, mert érinti a védekezéshez való jogot is: érdemes vajon megkockáztatni a visszahekkelést? Vagy egy digitális szabotázsakcióra, amelyet létfontosságú infrastruktúra ellen intéznek, harcászati nukleáris fegyverekkel válaszolni?

„Elképzelhető egy olyan cybertámadás, amely a NATO-szerződés 5. cikkelye értelmében támadásként értelmezendő, s mint ilyen hatályba lépteti a többi NATO-partner segítségnyújtási kötelezettségét? Úgy gondolom, a kérdésre szükségképpen igennel kell válaszolnunk. Ha pedig ez így van, az a nukleáris fegyverek bevetését is magába foglalná... Félelmetes elgondolás!”, állapítja meg aggodalmasan Wolfgang Ischinger.^[89]

Ami a hibrid támadások kezelését illeti, a világ továbbra is Amerikára függeszti majd tekintetét. Az amerikaiak ezügyben nem a galamb álláspontot teszik magukévá, és hajlanak arra, hogy egy hibrid támadást rendszerint gyorsabban minősítsenek háborús cselekménynek, mint az európaiak. Ezen az alapon ugyan a nemzetközi jog megengedne egy védelmi háborút – de egyáltalán ki az, aki ellen védekezni kell?

Az amerikai elnökválasztásokba való orosz beavatkozás kérdése ennek a bizonytalanságnak egy különösen kirívó példája. Vlagyimir Putyin cáfolt az elnökválasztási küzdelembe való minden beavatkozást, s úgy tűnik, Donald Trump szívesebben hisz neki, mint saját biztonsági szervezeteinek. Trump, nem is egy alkalommal, igen határozottan leszögezte, hogy az amerikai elnökválasztásokat bárki meghekkelhette – Észak-Korea, Kína,

Irán, sőt az a helyes New Jersey-i szomszéd fiú is. 2018. július 16-án az Oroszország és az Egyesült Államok közötti csúcstalálkozón tett nyilvános nyilatkozataival újra megerősítette álláspontját: „Az embereim felkerestek (...) és azt mondták, úgy gondolják, Oroszország az [amely a választásokba beavatkozott]. Beszéltem Putyin elnökkel; éppen most mondta, hogy nem Oroszország. Hadd fogalmazzak így: nem látom okát, hogy ne így volna.”^[90]

Aki hibrid támadás esetén nem képes ellencsapásra, mert nem állapítható meg, hogy támadásról van-e szó, és hogy egyáltalán ki hajtotta végre, elveszíti képességét a második csapásra; fenyegetése, hogy második csapása megsemmisítő erejű lesz, értelmét veszti.

A digitális potenciálok bővülésével párhuzamosan „a második csapás koncepció teljes szertefoszlásának vagyunk tanúi. Annak lehetősége, hogy viszonyozunk egy támadást, maradéktalanul megszűnik, mert nem tudunk védekező csapást végrehajtani”, állapítja meg ezzel kapcsolatban Jean-Marc Rickli.^[91] „Pedig a stratégiai egyensúly egész koncepciója az elrettentés gondolatára épül. Az elrettentésnek védelmi jellege van.”^[92] Ameddig Oroszország a hidegháború idején nem lehetett biztos abban, hogy lehetséges-e két egymás utáni támadást végrehajtani – azaz „először semlegesíteni az amerikai rakétasilókat, aztán pedig egy nukleáris csapást végrehajtani, vagyis amíg kétséges volt, hogy egy ilyen támadás működhessen –, addig stabil stratégiai egyensúly állt fenn.”^[93]

Az elrettentés korszaka tehát, úgy tűnik, véget ért, mert a digitalizáció itt is gondoskodik a diszkontinuitásról. Aki képes digitális támadást végrehajtani anélkül, hogy ellencsapással kellenne számolnia – mivel sikerül hatékonyan álcáznia magát, helyettesítőit az előtérbe tolnia és mindent cáfolnia –, felszámolja a stratégiai egyensúlyt. A hatalmi egyensúly a potenciális támadó javára tolódik el. Másfelől nézve ez azt jelenti – s ezzel feltárul Pandora szelencéje –, hogy a hibrid támadások ellen a legjobban úgy védekezhetünk, ha az első csapást mi mérjük az ellenfélre. „És az egyensúly a védelemtől egyszerre az első csapás irányába tolódik el.”^[94]

Megfontolásai során Jean-Marc Rickli egy sajátos digitális újdonságra, nevezetesen a támadó, autonóm módon cselekvő drónrajokra utal. A rajtámadással kapcsolatban mégsem kell azonban mindjárt drónokra gondolnunk. Egy DDoS (*distributed denial of service*), azaz egy osztott szolgáltatás-megtagadásos támadás számítógépek ellen, ami vállalkozásokat, hatóságokat vagy kritikus infrastruktúrát bénít meg, a megosztott cselekvést aknázza ki. Egy decentralizált, nem egykönnyen felismerhető, decentrális rendszer ugyanis stabilitás és túlélési esély tekintében fölényben van egy centrális rendszerrel szemben. Egy centrális rendszer kiiktatásához ezzel szemben elegendő egyetlen végzetes csapás.

Röviden: az a dinamika, amelynek a digitalizáció technológiai erői révén kitesszük magunkat, olyan kockázati közeget jelent, ami krízisekre hajlamos. És amire a mi jelenleg érvényes nemzetközi jogunk nem szolgál válasszal.

Adattolvajok

„A vádlottak (...) a GRU [orosz katonai titkosszolgálat] tisztjei voltak. Előre megfontolt szándékkal közösen és másokkal, a vádesküldtszék számára ismert és ismeretlen személyekkel (együttesen: »az összeesküvőkkel«) léptek titokban együttműködésre azzal a céllal, hogy felhatalmazás nélküli hozzáférést szerezzenek a 2016-os elnökválasztásokban érintett amerikai állampolgárok és jogi személyek számítógépeihez (»meghekkeljék« e gépeket), a számítógépekről dokumentumokat lopjanak, és az elloptott dokumentumokat a 2016-os elnökválasztások megzavarása céljából nyilvánosságra hozzák.»^[95]

Jelen esetben az összeesküvők elleni, 2018. július 13-i vádirat rendkívül kényes politikai tartalommal rendelkezett. Az Igazságügyi Minisztérium különleges ügyésze, Robert Mueller munkájának közbenső eredményeként született meg: tizenkét orosz ellen emeltek benne vádat az amerikai választási küzdelembé való beavatkozás, számítógépes bűncselekmények és pénzmosás miatt.

Már a második ilyen vádirat volt. 2018 februárjában is megvádoltak tizenhárom orosz, köztük „a Kreml szakácsát”, Jevgenyij Prigozsint, akinek *Konkord* nevű gasztronómiai vállalkozása fedőcégül szolgált orosz hibrid tevékenységekhez. A dokumentum szerint megtévesztés céljából avatkoztak be az amerikai kormányzat működésébe.^[96]

A más államok politikájába való beavatkozás nem új dolog. Már a predigitális időkben is megpróbáltak bizonyos országok

hatalomváltást előidézni más országokban, nem riadva vissza sem a puccstól, sem az ásványi kincsek vagy az állami pénzügyek gazdasági kontrolljától, sőt, a gyilkosságtól sem.^[97] Mueller mostani vádirata példásan írja le egy olyan állam tevékenységét, amely a 21. századi digitális hálózatiságot célzottan, stratégiaileg és taktikailag arra használja fel, hogy saját hasznára beleavatkozzon egy másik nemzet kormányalakításába.

Mueller vádjait a jövőbeli hibrid támadások elhárítása szempontjából az teszi igen értékesé, hogy részletesen leírja, hogyan hekkelték meg, hogyan fosztották ki, és hogyan fertőzték meg kártékony szoftverekkel az orosz katonai hírszerzés munkatársai a demokraták számítógépeit. Sikerült betörniük az amerikai Demokrata Kongresszusi Kampánybizottság, a *D-trip (Democratic Congressional Campaign Committee)* gépeibe, és Hillary Clinton választási kampányfőnökének, John Podestának (Bill Clinton egykori kabinetfőnökének) e-mail-fiókjába. A vádlottak, így az összefoglaló, a demokrata kampánystáb munkatársainak tucatjait figyelték meg, s a tőlük eltulajdonított dokumentumokat 2016 júniusa és novembere között hamis internetes identitásokat felvéve közzétették – 2016. október 7-én pedig az „Organisation 1” segítségét is igénybe vették. Ez utóbbi nyilvánvalóan utalás a WikiLeaksre. A vádlottak, hogy leplezzék Oroszországgal való kapcsolatukat, hamis identitásokat vettek fel, globális eloszlású rendszerek számítógépeit bérelték ki, titkos műveleteik költségeit pedig a bitcoin kriptovalutában fizették.

Senkinek, aki bitcoinnal fizet, nem kell bankkal kapcsolatba lépnie. Nem kell sem igazolnia magát, sem alávetnie magát a

pénzintézetek a pénzmosást megakadályozni hivatott szigorú jogosultsági vizsgálatainak. A bitcoint ugyanis a hasonló gondolkodású felhasználók cserebörzsein szokás beszerezni, netán mit sem sejtő komputer-felhasználók eszközeinek manipulációjával, ezek processzor-teljesítményének megcsapolásával, bitcoin-szerzés céljából.

A vádlottak, hangzik a folytatás, mintegy 95 ezer dollárt mostak át ezen a módon, és pénzátutalásokat indítottak külföldről az Egyesült Államokba, hogy ily módon ottani illegális tevékenységeiket finanszírozzák. Ezeket Müller részletesen bemutatja:

A vádlottak legkésőbb 2016 márciusától hamisított e-maileket kezdtek küldeni 300 amerikai célszemélynek: ezt a műveletet nevezik *social engineering*nek is. Ezeknek az adathalászatra bevetett (phishing) maileknek az volt a célja, hogy gyanútlan célszemélyeiket rábírják jelszavaik kiszolgáltatására. És csak ugyan: az oroszok már 2016. március 19-én nagy fogásra tettek szert. John Podesta elektronikus postafiókjába is érkezett egy phishing üzenet. Hillary Clinton választási kampányfőnöke, a Fehér Ház valamikori kabinetfőnöke készpénznek vette, hogy az e-maillal a Google előzékenyen közli: egy jogosulatlan személy hozzáfért Google-fiókjához. Mivel az IT-gigász időközben szigorította biztonsági protokollját, egy ilyen e-mail nem volt eleve gyanús. Ajánlják Podestának, hangzott az üzenet, hogy változtassa meg elektronikus postafiókjának jelszavát. Aki azonban az e-mailben látható linkre kattintott, semmiképpen sem a Google-hoz jutott tovább, a link ugyanis egy hamisított weboldalra

nyílt, amely mindössze hihetően utánózott egy Google-oldalt. Aki itt megadta Google-jelszavát – „Írja be régi jelszavát!” –, kulcsot adott az orosz titkosszolgálat kezébe saját e-mail-fiókjához. Ezek után a trükkös csalóknak alig két napra volt szükségük ahhoz, hogy lemásoljanak több mint 50 ezer e-mailt John Podesta e-mail-kontójáról.

A vádlottak phishing hadjáratáról azonban később kiderült, hogy mindössze hídfő létrehozását célzó művelet, egy nagyobb terv része volt. Miután sikerült behatolniuk az áldozatok Google-fiókjaiba, a már károsultak komputereihez való hozzáférést arra használták, hogy biztonsági réseket keresve kutakodjanak az egyes számítógépekben, illetve a demokraták számítógépes hálózatában. IP-címeket és hálózati konfigurációkat fürkészték ki, hogy feltérképezzék a hálózatba kapcsolt készülékeket. Ez azután megkönnyítette az X-Agent kártékony szoftver becsempészését, amely képes volt regisztrálni, hogy a billentyűzet mely gombjait nyomják le, és képernyőfotókat is tudott készíteni. Több szerveren keresztül, többek közt egy Atlantában kibérelt gépen át áramlottak a *keylogging*- és *screenshot*-adatok az orosz vádlottakhoz, többek közt a demokraták egyik választási adománygyűjtési akciójának banki adatai is.

Az áldozatok megfigyelése nem korlátozódott pusztán a felhasználók komputer előtti magatartására. Az oroszok célzottan hozzáláttak, hogy áldozataik számítógépeit minden lehetséges fontos információ után átkutassák. Bizonyosan találtak is ilyeneket. A fájlok közt, amelyek a kezükbe kerültek, előfordultak a 2016-os elnökválasztással kapcsolatos taktikai tervek, és egy

mappa, amely a „Benghazi-vizsgálatok”^[98] címet viselte. Ahhoz, hogy az adatok e tömegeit észrevétlenül, ugyanakkor titkosítva küldhessék át szervereik egyikére, kis terjedelemben tömörítették az adatokat, és törölték a kifosztott számítógép eseménynaplóját. Ehhez igénybe vették az ingyenes CCleaner törlőprogramot is. Ha még titkosszolgálatok is az ingyenes brit tisztítóeszközhöz folyamodnak, ismét csak megerősítik az információtechnológiai szakma legnevesebb médiavállalatainak értékelését, amely szerint a CCleaner világszerte a legjobb nyommegsemmítők közé tartozik.

A demokraták csak 2016 májusának végén fedezték fel, hogy meghekkelték őket. A rákövetkező hónapban egy biztonsági cég foglalkozni kezdett a problémával, és kikapcsolta az X-Agent megfigyelőprogramot a számítógépeken és a demokraták hálózatán. A vádlottak immár nem voltak abban a helyzetben, hogy kapcsolatba lépjenek kártékony programjukkal, a kudarc azonban nem tartotta vissza őket attól, hogy másféleképpen szerezzenek politikai információt: pótlékképpen a demokraták infrastruktúra-szolgáltatóját vették célba. A felhőszolgáltató számítógépeire, amely weboldalán az *Elections as Service* („Választások mint szolgáltatás”) szlogennel hirdeti magát, és konkrét példaként a Demokrata Nemzeti Bizottságnak (DNC) nyújtott szolgáltatást ismerteti,^[99] a bizottság egy választási adatokat elemző tesztalkalmazást telepített, amely alkalmas volt annak megállapítására, hogy a választásra jogosultak közül előreláthatólag kik fognak majd Hillary Clintonra szavazni. Ezt az új célpontot derítették fel a vádlottak, majd saját számítástechnikai központról

készített saját másolatukkal készítettek egy „pillanatfelvételt” a DNC-adatokról, és saját fiókjaikba helyezték át, amelyet ugyanannál az üzemeltetőnél létesítettek.

A vádlottak hagytak maguk után egy hamis nyomot is, hogy eltereljék magukról a gyanút. „Idegen zászló alatt végrehajtott akciónk”-hoz (*False flag operation*) létrehoztak egy Guccifer 2.0-nak elnevezett hamis online identitást, és azt a látszatot keltették, hogy az nem más, mint egyetlen román hekker, egy magányos farkas, akinek sikerült a nagy húzás, hogy támadást intézen fontos amerikai számítógépek ellen.

Guccifer 2.0 valamivel később még igen fontos szerepet játszott ebben a sajátos választási krimiben. Ez volt ugyanis az a hamis identitás, amely utóbb közvetlenül kommunikált a választókkal és az amerikai politikusokkal is.

Kritikus infrastruktúrák veszélyben

„A figyelmeztető lámpák ismét pirosan villognak”, véli Dan Coats, az amerikai titkosszolgálatok országos koordinátora, volt németországi amerikai nagykövet.^[100] Miként a 2011. szeptember 11-e előtti hónapokban is, mondja, az amerikai titkosszolgálatok riasztó aktivitást észlelnek, ennek alapján pedig az Egyesült Államok egy esetleges támadásnak van kitéve. „Országunk a digitális infrastruktúrájára szó szerint pergőtűz zúdul.”^[101] Oroszország és más szereplők – Coats néven nevezi Kínát, Iránt és Észak-Koreát, de utal terroristákra és bűnözőkre is –, mint

mondja, kihasználják a kritikus infrastruktúra sebezhetőségét, hogy behatoljanak amerikai energetikai hálózatokba, a vízellátásba, a nukleáris létesítményekbe és a feldolgozóiparba. Nem sok hiányzik, állítja, hogy katasztrófát idézzenek elő – a politikai akaraton kívül, hogy lenyomják a kritikus gombot.

Tehát, ahogyan ezt vádiratában Robert Mueller részletesen bemutatta, manapság számos digitális támadást hajtanak végre. Dimenziójuk, hatótávolságuk és súlyos következményeik az államok közti hatami viszonyokra és a társadalmi normákra riasztotta a nemzetek irányítóit. A kormányok immár nem riadnak vissza attól, hogy nyíltan megfogalmazzák vádjaikat a hibrid támadásokat illetően. A 2018-as Müncheni Biztonsági Konferencián az Egyesült Államok, Kanada és Ausztrália mellett Dánia és Nagy-Britannia is felrótta Oroszország kormányának, hogy ő a felelős a WannaCry programkódjából származó NotPetya zsarolóprogrammal végrehajtott támadásért. Az oroszok tagadták. Miközben a WannaCry-támadás 2017 májusában első ízben sodort veszélybe emberéleteket, mert lehetetlenné tette, hogy brit kórházak felvegyék és kezeljék pácienseiket, az ez után következő, 2017 júniusi NotPetya-támadás súlyos gazdasági károkat okozott. Egyedül csak a Maersk hajózási társaság 50 ezer számítógépét volt kénytelen újrainstallálni,^[102] aminek költsége több száz millió dollárra rúgott. A javítások körülbelül tíz napos időszakában a Maersk arra kényszerült, hogy ügyeit manuálisan, papíron adminisztrálja. Feltételezik, hogy a NotPetya, amelynek vélhetően kifejezetten Ukrajnát kellett volna megkárosítania, világszerte milliárdos nagyságrendű károkat okozott.

Nem minden elképzelhető, technikailag kivitelezhető vagy már előkészített forgatókönyv következik be ténylegesen. Ez azonban mit sem változtat azon, hogy kockázati környezetünk mindannyiunk hátrányára változik meg, mert akadálytalanul terjed a *minden internetje*, a környezeti intelligencia technológiájának hordozója. Az autókat, házakat, munkahelyeket és magukat az embereket is egyre több monitoring-technológiával szerelik fel, hálózatokba kapcsolják, drót nélküli kapcsolaton keresztül irányítják és optimalizálják, ahogyan az ipari létesítményeket és a kritikus infrastruktúrákat is. Gazdasági okokból akarja így a politika.

A környezeti intelligencia azonban újabb nagy biztonsági kihívást jelent majd. Egyelőre még számos eszközt az IPv4, az internet negyedik verziója köt össze. Az olyan készülékek, mint a nyomtatók, a laptopok vagy IP-telefonok ma egy közös hálózati routerhez kapcsolódnak, mert a rendelkezésre álló IP-címek száma korlátozott. A router összekapcsol és továbbít, de a számítógép-hálózatban tűzfal-szereppel is rendelkezik. Hardvervédelmet jelent, s ekként a szoftveres védelem mellett második biztonsági mechanizmusként szolgál az ellen, hogy egy hálózathoz vagy egyes gépekhez illetéktelenek engedély nélkül hozzáférjenek. Ha azonban még inkább elterjed majd az IPv6-szabvány, minden egyes számítógép és hálózati végpont, minden szenzor és vezérlés saját, egyértelműen azonosítható IP-címmel rendelkezik majd, s közvetlenül, router nélkül, és ennél fogva hardveres védelem nélkül kapcsolódik majd a nyílt, védelem nélküli internethálózathoz.

A digitális sebezhetőség azonban az IPv6 nélkül is sok esetben visszavezethető a felhasználók könnyelműségére. A gáztermelés létesítmény-üzemeltetői örülnek, ha módjukban áll a világ különböző pontjain működő gyáraik központi létesítményvezérléséhez „okostelefonon a tópartról is hozzáférni”.^[103] A német közlekedési infrastruktúra működtetőinek semmi gondjuk azzal, hogy az adatok, amelyeket a szenzorok a német utakról összegyűjtenek, titkosítatlan formában továbbítódnak egy amerikai számítóközpontba – ugyanahhoz az infrastrukturális vállalkozáshoz, amely szolgáltatásként kínálja a választásokat, és amelyet az amerikai elnökválasztások során nyilvánvalóan meghekkeltek. „Bárki odaállhat az útpálya mellé, és láthatja milyen állapotban van. Ezt az információt nem kell titkosítva továbbítani.”^[104] Így és hasonlóképpen hangzanak a német vállalkozók naiv, vállrándító válaszai, amikor figyelmeztetik őket az esetleges hekkertámadásokra, illetve annak veszélyére, hogy harmadik fél adatokat tulajdoníthat el a számítóközpontokból.

Az észérvek ez esetben sajnos nem segítenek, s ennek egyszerű a magyarázata. A környezeti intelligencia felhasználói élvezni akarják a működőképességet, a kényelmet és az automatizálást. Ezért a digitális termékeket vagy szolgáltatásokat kínáló palettájukat a funkcionalitásra összpontosítva alakítják ki. A funkciót ugyanis el tudják számolni. Ezért van az, hogy minden szolgáltató bizonyítani tudja a funkcionalitás rentabilitását: hogy mennyi pénzt képes megtakarítani a felhasználó egy bizonyos funkcióval, hogy milyen anyagi előnnyel jár a számára egy funkció, s hogy ebből mekkora részt könyvelhet el haszonként.

Hogyan mérhető azonban az a megtakarítás vagy nyereség, ami a nagyobb biztonságból származik? A biztonság jövedelmezőségének először be kell bizonyosodnia. Noha a tanácsadó cégek jó indokokkal szolgálnak arra nézve, hogy a szolgáltatóknak és a felhasználóknak is miért kellene pénzt kiadniuk a biztonságra, ám a biztonság immateriális érték, és többbe kerül, mint amennyit hoz. Demonstratív példa erre az, ami a Facebookkal 2018. július végén történt. A vállalat egyetlen kereskedési napon nagyjából 123 milliárd dollárt – avagy tőkepiaci értékben mintegy 20 százalékot – veszített, amikor figyelmeztette az érdekelteket, hogy forgalma a vártnál kisebb lesz, ekképpen pedig kitudódott, hogy az adatlopás, a gyűlöletbeszéd vagy a *fake news*, a kamu hírek elleni további védekezés nagyon sokba fog kerülni – ráadásul úgy, hogy ugyanakkor a felhasználók számának csökkenése várható.^[105]

A felhasználók kimondatlanul elvárják, hogy a környezeti intelligencia biztonságos legyen, de jobb, ha erre nem számítanak túlságosan. A rendszermérnökök arra figyelmeztetnek, hogy a biztonságot már egy digitális ajánlat megtervezésénél sem veszik figyelembe: a felhasználónak a biztonságra tekintettel lévő tervezés vagy biztonságosra tervezés (*safety-by-design* és *security-by-design*) iránti igénye áldozatul esik a funkcionalitás-többletnek, és nem is veszik tekintetbe kellő mértékben.^[106] Ha azonban már megterveztek és elkészítettek digitális terméket, nehéz vagy akár lehetetlen növelni a biztonságosságát.

Mindezek után Ehud Schneorson, az izraeli hadsereg titkoszolgálatának, a 8200-as egységnek egykori vezetője azt prog-

nosztizálja, hogy minden jövőbeli háború legfőbb célpontja egy állam kritikus infrastruktúrája lesz. „Az energetikai infrastruktúra a modern nemzet szíve és vérkeringése”, állapítja meg. Egy támadás ez ellen az infrastruktúra ellen előnyöket biztosítana, és digitális 9/11-gyé válhatna.^[107] Ezzel Ehud Schneorson ugyanazt a véleményt képviseli, mint amerikai kollégája, Dan Coats.

Az ellenfelek még nem csaptak le, felkészülni azonban felkészültek. Vajon egészen pontosan mit vesznek célba?

Hibrid támadások célkeresztjében

Jóllehet az USA-ban külföldről eddig csak energetikai hálózatokat és áramszolgáltatókat támadtak, ez messze nem nyugtathatja meg Németországot. Amikor tudniillik észlelték, hogy a Berserk Bear hekkercsoport mindenütt jelenlévő fenyegetést jelent a német villamossági hálózatok és energetikai vállalkozások számára, a Német Információtechnika-biztonsági Hivatal (BSI) és az Alkotmányvédelmi Hivatal (BfV) riadót fűjt. Már évek óta észleltek támadásokat a német infrastruktúra ellen, most azonban a támadók jogosulatlan vezérlési utasításokat küldtek routerekre, hogy a hálózat elemeit a hálózat konfigurációs részleteinek leszívására késztessek, és hozzáférési adatokat halásszanak le.^[108] Úgy tűnik azonban, irodai hálózatoknál nem hatoltak mélyebbre.

„A választott módszer valójában annak a számos bűnjelnek az egyike, amelyek a támadáskampány orosz irányítására utalnak”, pontosított D. Hans-Georg Maaßen, az Alkotmányvédelmi Hivatal volt elnöke a támadók módszereit illetően.^[109]

„Betörtek a hálózatainkba, és korlátozott vagy kiterjedt támadásra pozícionálják magukat”, véli az amerikai Michael Carpenter, az amerikai védelmi miniszter korábbi helyettes államtitkára. „Fedett háborút viselnek a Nyugat ellen.”^[110]

„Nagyon világos különbséget tennék a hibrid fenyegetés és a hibrid háború között”, veti azonban ellen nyomatékosan Hans-Georg Maaßen.^[111]

Feltűnő, mennyire különbözik a két magas rangú államhivatalnok szóválasztása – amiként aktuális vagy korábbi állami pozíciója is.

„A háborút mint állapotot egyáltalán nem szükséges taglalnunk, hisz végső soron definiálja a nemzetközi jog, függetlenül attól, hogy hadüzenetet követően, vagy anélkül kerül sor rá”, fejt ki részletesebben a német alkotmányvédelem korábbi elnöke.^[112] „Hibrid háború esetén rendszerint érzékelhető hadiállapottal van dolgunk, amelyet hibrid intézkedések kísérnek. (...) Hibrid fenyegetettség esetében békeállapottal van dolgunk. Az érintettek egyikének sem áll szándékában, hogy a másiknak hivatalosan hadat üzenjen, vagy hogy csapatokat vonultassanak fel egymás ellen. Ellenkezőleg, a cél annak elkerülése, hogy valaki nyíltan ellenséges szándékú ellenfélként lépjen színre.”^[113]

A német alkotmányvédelem volt elnöke egy civil hatóság élén állt, az amerikai Carpenter a hadügyben dolgozott. Ez nem

csak a hibrid támadásokhoz való viszonyulásukat alapozza meg és formálja. Ha digitális támadások elhárításáról van szó, az amerikaiak agresszív héjákként nyilvánulnak meg. Ám a környezeti intelligenciákat érő támadások esetében is nem utolsósorban az illetékesség meghatározásán fordul a kocka. A háború fogalma ugyanis egyértelműen kijelöli egy meghatározott hatóság illetékességét. „Abban a pillanatban, amikor »háborúnak« nevezhetek valamit, a fegyveres erők illetékességével van dolgom”, állítja Heiko Borchert, fegyverkezési együttműködéssel, energetikai biztonsággal és geostratégiai elemzéssel foglalkozó biztonsági és védelmi tanácsadó.^[114] „Végül is szükséged van egy címkére, amely politikailag tolerálható és elfogadott, s amelynek birtokában megtehetsz dolgokat.”^[115]

A digitális támadásoknak egy másik államtól kiinduló hibrid fenyegetésként való besorolása viszont a német alkotmányvédelmet hozza helyzetbe.

„A belföldi biztonsági hatóságok feladata, hogy foglalkozzanak a hibrid támadásokkal”, mondja Hans-Georg Maaßen. „Elképzeltetik, ennyire nagy kihívás ez a Szövetségi Alkotmányvédelmi Hivatal számára, mivel egy hibrid fenyegetés esetén a velünk szemben álló úgy jár el, mintha háborút viselne, de anélkül, hogy valaha is hadiállapotot akarna hirdetni. Az ellenfél a háborús küszöb alatt tevékenykedik, óvatosan és finoman, a hatóságok pedig, amelyeknek ezeket a támadásokat ki kellene védeniük, polgári hatóságok.”^[116]

Az illetékességek kérdésével a későbbiekben foglalkozunk még. Különös jelentőségre akkor tesz szert, amikor a hibrid tá-

madások elleni védelem jogi lehetőségekről van szó.

Térjünk azonban vissza a támadások célpontjaihoz. Potenciálisan veszélyeztetett az észak-atlanti **mélytengeri kábel**. Mivel az orosz haditengerészet jelentős beruházások árán bővítette, illetve továbbfejlesztette tengeralattjáró-flottáját, és az Atlanti-óceán északi térségében, az adatkábelek feltűnő közelségében olyan aktív, mint utoljára a hidegháború idején volt, a NATO aggodnik. Ha elvágnák az Egyesült Államokat és Európát összekötő kommunikációs összeköttetést, felbecsülhetetlen gazdasági károk keletkeznének. Valószínűbb azonban, hogy az orosz tengeralattjárók megcsapolják a kábelt, és az adatokat – nyaralásokon készült ártalmatlan fotóktól szellemi tulajdonon át a pénzügyi tranzakciókig – elemzés céljából anyahajóikra továbbítják. Sok minden erre a forgatókönyvre utal, miután az Egyesült Államok 2018 nyarán gazdasági szankciókat hozott több orosz vállalkozás ellen. Azzal vádolták őket, hogy szorosan együttműködnek a Kremlllel. A szankcionált cégek közé tartozik a Divetechnoservices vállalat is, amelynek azt rótták fel, hogy tengeri kábelek lehallgatására szolgáló technológiákat állít elő.^[117] Ha ez igaz, akkor egy alapjában gyanún felül álló, kereskedelmi jellegű tenger alatti berendezéseket gyártó cég is alkalmas helyettesítője lehet az állam haditengerészetének.

Ha tenger alatti kábelek lehallgatása során pénzügyi tranzakciókkal kapcsolatos információkat is támadás ér, a G20 államok pénzügyminiszterei és központi bankjaik elnökei idegesek lesznek. Már 2017-es baden-badeni találkozójukon figyelmeztettek: az információs- és kommunikációs technológiák rosszhi-

szemű alkalmazása alááshatja a **globális pénzügyi rendszer** biztonságát és a belé vetett bizalmat, és veszélyeztetheti az államok pénzügyi stabilitását.^[118] 2007 óta már jó néhány súlyos, pénzügyi intézmények ellen végrehajtott támadást regisztráltak, köztük DDoS-támadásokat, pénzlopást vagy piacok és adatok manipulálását. Alaposabb vizsgálatok mindazonáltal arra utalnak, hogy habár a kereskedelmi bankok, tőzsdék és központi bankok elleni támadások gyakran politikai motivációjúak voltak, kevés kivétellel mégiscsak bűnügyi indíttatásból követték el őket, nem pedig államok álltak mögöttük.^[119] E kivételek közé tartozik Észak-Koreának a bangladesi központi bank elleni, 2016 februárjában végrehajtott támadása, amelynek során az elkövetők eredménytelenül igyekeztek eltulajdonítani egymilliárd amerikai dollárt, azaz Banglades bruttó nemzeti termékének 0,58 százalékát.^[120] Oroszország is több alkalommal lett pénzügyi rendszere ellen irányuló támadásoknak az áldozata. A globális pénzügyi stabilitásba vetett bizalmat megőrzendő ezért a G20 államoknak határozott szándékuk, hogy ha ilyen fenyegetések adódnának – önkéntes konvenció alapján – a globális pénzügyi rendszer vonatkozásában, lemondanak a hibrid technikákról, és együttműködnek egymással.^[121]

Nem áll azonban ugyanez a **televízióra**, amely továbbra is sebezhető. 2015. április 8-án meghekkelték a francia TV5 Monde tévéadót, amelyet három órán át teljesen működésképtelenné tettek. A támadást a CyberCaliphate vállalta magára. Míg régebben írásban ismerték el az ilyesmit, elegendő erre ma egy *defacement*, az áldozat weboldalának eltorzítása a beismerő nyilat-

kozat globális elterjesztésére. Ezúttal a francia csatorna elleni támadással egy időben annak Twitter- és Facebook-fiókjait is meghekkelték. Az eltorzított imázs képen immár a „Je suIS IS” (Én az Iszlám Állam vagyok) szöveg volt olvasható, alatta pedig a következő szöveg: „Franciaország katonái, tartsátok távol magatokat az Iszlám Államtól! Lehetőségetek van rá, hogy a családokkal maradjatok, használjátok ki!” Különösen aljas és az érintettek számára magas kockázattal járó lépés volt, hogy a meghekkelt közösségimédia-oldalakon francia katonák rokonainak személyes adatait posztolták, együtt egy Hollande-hoz, a volt kormányfőhöz intézett figyelmeztetéssel, mely szerint a 2015 januári, párizsi terrorakciókat mindössze ajándéknak szánták terrorellenes háborújáért.

Hosszan tanakodtak az Iszlám Állam digitális képességeivel kapcsolatban. Vajon képes lenne az IS digitális támadás végrehajtására?

„Természetesen az IS-nél is akadtak egyes személyek, akiknek volt affinitásuk az információs technológiához. Megfigyeltük, hogy képesek voltak DDoS-támadásokat szervezni, hogy hozzáférésük volt hekkercsoportokhoz, és hogy rendelkeztek potenciállal *defacement*-akciók végrehajtására”, fejti ki Hans-Georg Maaßen.^[122] „Nem tudtuk azonban megállapítani, hogy az IS-nek vannak-e emberei, know-how-ja nagyobb szabású cyberrattakokhoz.”^[123]

Az olyan összehangolt támadás azonban, amilyen a TV5 Monde elleni volt, gondos tervezést tett szükségessé, ennél fogva nagyon is követhette el másvalaki, mint az IS. Vajon a támadó

csak álcaképpen öltötte magára az IS identitását, egy „idegen zászló alatt végrehajtott művelet”-hez? A francia hatóságok több hónapon át vizsgálódtak, mire meggyőző eredményre jutottak: a kártékony szoftver egy részét cirill betűs billentyűzeten készítették és orosz hivatali időben állították össze.^[124] A támadás ugyanattól a csoporttól származhatott, amelyik egy évvel később az amerikai demokratákat is meghekkelte, és amelyiknek nem is egy neve van – FancyBear,^[125] Pawn Storm vagy AP-T28 –, egy olyan hekkerszervezettől, amelynek valódi nevét senki sem ismeri. Ez arra utal, hogy még kormányzati szereplők helyettesítői is tudják magukat úgy álcázni, hogy ez tovább nehezítse egy támadás hozzárendelését egy kormányhoz.

Ugyanennek a szervezetnek róják fel a német Bundestag elleni 2015-ös, és a **kormányzati hálózatok** elleni 2018-as támadást.^[126] Noha a világ nyilvánossága kevesebb figyelmet szentelt nekik, még látványosabbak voltak a Montenegro kormánya elleni 2016/17-es digitális támadások. A mintegy 630 ezer lakost számláló kis balkáni állam maga akarta eldönteni, vajon az oroszokhoz, vagy inkább a NATO-hoz közeledjék. Donald Trump így jellemezte Montenegrót: „kis ország (...), amelyet nagyon agresszív emberek laknak”, és amely kirobbanthatná a harmadik világháborút.^[127] Már a EU- és NATO-párti, de 1991 óta hatalmon lévő, korruptnak tekintett Milo Đukanović, illetve az orosz-barát ellenzék közti választási küzdelmek során támadók akadályozták meg DDos-akciókkal a hozzáférést a kormány weboldalához, pontosan egy olyan az időszakban, amikor a választók különösen rá voltak utalva az adatokra és információkra, hogy

megfelelő értesülések birtokában hozhassák meg választási döntésüket. A montenegrói kormány digitális támogatással végrehajtott puccskísérlettől tartott, és október 20-án, a választás napján húsz szerbet vétetett őrizetbe, akiket azzal vádoltak, hogy egy külföldi kormány – a Kreml – szolgálatában összeesküvést szőttek Đukanović meggyilkolására. Az akció biztosította Đukanović hatalomban maradását, amin a kormány számítógépei elleni támadások sem tudtak változtatni.

Amikor Montenegro 2017 februárjától formálisan is közeledett a nyugati katonai szövetséghez, a támadások ismét megsohasodtak és súlyosabbá váltak. Különösen a 2017. június 5-i NATO-csúcs előtt „állt heves, kíméletlen támadások keresztüzében a kormány infrastruktúrája, ami igazi kihívást jelentett számunk számára”, ismerte el a montenegrói információs biztonsági szervezet főigazgatója, Milica Janković.^[128]

A teljes hálózatiság korszakában különösen nagy kihívássá lett a **fegyverrendszerek** biztonsága, nevezetesen akkor, amikor a nukleáris robbanótesteket mind jelentősebb szenzorikával szerelik fel, és hálózatokhoz csatlakoztatják. Ez okból a fegyveres erők digitális szempontból már régóta a fegyverzet vezérlését, vagy az ellenséges állások felderítését szolgáló környezeti intelligencia terén mutatják a legnagyobb előrehaladást. A katonai rendszereknek a jogosulatlan beavatkozások elleni biztosítása azért is még egy fokkal fontosabb, mert Donald Trump amerikai elnök az Egyesült Államok atomarzenálját körülbelül a tízszeresére akarja növelni, ekképpen pedig egyértelműen el-

határolódik elődje, Barack Obama víziójától, aki maradéktalanul denuklearizálni akarta a világot.^[129]

Különösen veszélyeztetettek a fegyverrendszerek irányítórendszerei és a kommunikációjuk, ezek nem csak meghekkelhetők, hanem *spoofol*hatók és *jammel*hetők is. Az első esetben egy mérési érzékelőre hamis adatokat küldenek, a második esetben „elektronikus zavaró tűz” akadályozza meg, hogy egy szenzor egyáltalán mérési adatokra tegyen szert. *Electronic warfare*-ről, elektronikus hadviselésről van szó. A támadás célpontja ez esetben a láthatatlan elektromágneses tartomány, azok a rádióhullámok, amelyek nélkül a 21. századi mindennapokban már semmi sem lehetséges. Katonai területen az elektromágneses spektrumot például nagy hatótávolságú precíziós fegyverek, legújabb generációs harcjárművek és ember nélküli robotok irányítójel-átviteli közegeként alkalmazzák – ezen kívül pedig a hiperszonikus fegyverek elleni rakétaelhárító fegyverek vezérlésére is.

Az elektromágneses tartomány egyre jobban megtelik hullámsávokkal, és égetően szükségessé vált, hogy ezt ne csak megtörténni hagyják, hanem aktívan menedzseljék is. Egy konfliktus alkalmával ezért valamelyik fél mindig meg fogja próbálni, hogy megszerezze az elektromágneses tartomány feletti ellenőrzést, hogy időlegesen megbénítsa az ellenfelet. Épp a katonák digitális eszközökkel való felszerelése során gondoskodni kell arról, hogy ne sugározzanak világítótorony módjára, s ne éppen jeleket kibocsátó felszerelésük miatt váljanak az ellenséges elektromágneses harcosok könnyű zsákmányává. Aki a csa-

tatéren hálózathoz kapcsolódik, annak képesnek kell lennie kibocsátott jelegyütteseinek leplezésére és a beérkező jelek visszaverésének elkerülésére, hogy lehetőleg észrevétlen maradjon.

A *spoofing* és a *jamming* egyaránt régóta ismert technika. A radartechnológia II. világháborús bevetése óta a konfliktusokban szembenállók mindig is próbálták zavarni az ellenfél elektromágneses spektrumát, hogy egy fegyveres támadás alkalmával észrevétlenek maradjanak, vagy pedig hogy az ellenfél egy támadása előtt felfedezzék és semlegesítsék annak fegyvereit. Manapság nagy a kereslet az *improvised explosive device*-okra (IED), az olyan csapdaszerű robbanóeszközökre, amelyek okostelefonos rádiótávírányítással a távolból is működésbe hozhatók, s amelyeket terroristák, lázadók vagy felkelők alkalmaznak az iraki vagy az afganisztáni háborúban. Akcióik során az amerikaiak sok IED-t tudtak ártalmatlanná tenni a levegőből, mivel célzottan zavarták a rádiójeleket, amelyeknek a robbanást elő kellett volna idézniük.

A *spoofing* és a *jamming* nemcsak katonai kontextusban jelent komoly fenyegetést: ezek a technikák a polgári mindennapokban is jelentős károkat okozhatnak. Amikor az ipari létesítmények üzemeltetői érzékelőket csatlakoztatnak levegőbontó, valamint lepárlóberendezéseikhez, gátjaikhoz, csővezetékeikhez vagy villamos hálózataikhoz, amelyek regisztrálják a létesítmény állapotát, majd elektromágneses hullámhosszokon információkat küldenek róla egy irányítóközpontba, *spoofing* esetén ez a központ hamis információkat kaphat a létesítményről. Ha

egy üzemeltető ezután távvezérléssel, ahelyett, hogy kinyitná, elzár egy szelepet, vagy ahelyett, hogy lelassítaná, felpörget egy kompresszort, azt kockáztatja, hogy „tönkrehajtja” a berendezését.

Míg az Egyesült Államokban „siló”-formában – azaz a katonai összecsapás sokelemű változataként – honosodott meg az elektronikus harc, Oroszország egyetlen holisztikus koncepcióba integrálta az elektronikus harcot, az ellenséges infrastruktúrák elleni támadásokat és az információs térben ezeket kísérő lépéseket. Ezért aztán egyetlen orosz dokumentumban sem fordul elő a „hibrid” fogalom, hiszen az orosz fegyveres erők eleve egy integrált, holisztikus szemléletet alkalmaz, s ezzel Oroszország megkülönbözteti magát a Nyugat eljárásmodjától, amelynek államai majd csak lassan állnak át integrált cselekvésre.

Vajon miért gyanúsítják Kínát ilyen ritkán azzal, hogy kezdeményezője más államok ügyeibe való, gyakran politikai indíttású beavatkozásoknak? Hiszen Kína rendelkezik olyan technológiai és pénzügyi lehetőségekkel, amilyenekkel Oroszország nem. A különbség a szándékokban rejlik. Vlagyimir Putyin korának gyermeke, és a Szovjetunióban, a mindenki mást ellenségnek nyilvánító marxista ideológia közegében szocializálódott. Lélekben igencsak megsebezte, amikor a Szovjetunió a 20. század kilencvenes éveiben széthullott, s most arra törekszik, hogy ismét olyan naggyá tegye Oroszországot, amilyen valaha volt. Ez megmagyarázza, hogy Putyinnak valószínűleg miért fűződik érdeke demokrata ellenfeleinek gyengítéséhez, miért akar éket verni az európai partnerállamok közé, illetve táma-

dást intézni a demokrácia ellen – amikor például megzavarja külföldi választások integritását, vagy jelölteket hiteltelenít.

Ezzel szemben Kína mindeddig csak adatlopásban volt érdekelt. „Kína know-how-t akar lopni. Ők termelni akarnak”, mondják az amerikai titkosszolgálat köreiben.^[130] A levegőben van azonban, hogy ez igen gyorsan megváltozhat.

[KETTŐ]

Információs háború

Az igazságon túl már a fasizmus előtt vagyunk. (Timothy Snyder)

Wolfgang Ischinger nyugalmazott nagykövet, a Münchener Biztonsági Értekezlet vezetője alaposan ismeri a német és európai biztonságpolitika kérdéseit. Mielőtt összehívna a biztonságpolitikuskor nemzetközi tanácskozását, világszerte tudakozódik szakmája művelőinek körében, hogy szerintük a külpolitika mely témaival kapcsolatban várható, hogy esetleg kihívássá válnak a nemzetközi biztonságra nézve. A válaszadás nagy politikai jártasságot tesz szükségessé, valamint ösztönös ráérzést és azt is, hogy valaki olvasni tudjon a jósok kristálygömbjében.

Aki tudja, milyen bonyolult viszonyokat eredményez egy nagy mértékben hálózatosított társadalom, nyomban megérti, hogy 2017 decemberében egy müncheni rendezvényen Wolfgang Ischinger miért nem tehetett mást, mint hogy megállapítsa: a külpolitika mindig is bizonytalan valami volt, ám néhány év óta kevésbé kiszámítható, mint valaha. A krízis jellegű események többé nem láthatók előre, és meglepetésszerűen következnek be.^[1] Egy ilyen közegben, folytatja Wolfgang Ischinger, a

geopolitikai világhelyzet olyan sokféle kockázatnak van kitéve, és olyan veszélyes, amilyen a Szovjetunió széthullása óta még sosem volt. Úgy tűnik, a politika most egyértelműen érzékeli a világ multipoláris újrafelosztásának dinamikáját: ebben a világban egyesek hatalma növekszik, másoké elenyészik. Ez a kiszámíthatatlanság, hangzik Wolfgang Ischinger igencsak jogos végkövetkeztetése, megnehezíti a jó külpolitika folytatását. Ezután a diplomata felsorolja „a politika bomlási tüneteinek” okait, köztük egy új jelenséget: az igazság elvesztését.

„Korábban – idézi fel Wolfgang Ischinger – megkülönböztettünk tényeket és meséket. Időközben a különbség immár nem ismerhető fel. Még Donald Trump munkatársai is arról beszélnek, hogy vannak tények és alternatív tények. Az igazság megállapításának akadályozását a külpolitikuskok közül a stratégiák így nevezik: *weaponization of information* [az információ fegyverként való alkalmazása]. Az információs tér maga is fegyverré lett.”^[2]

Semmi sem olyan, mint volt: az új normális

„Nem. Ön jön. Nem maga! A maguk szervezete kész fürtelem! Egyetlen kérdésére sem fogok válaszolni. Csönd. Ön van soron. Ne legyen már faragatlan! Maguk csak kamuznak.”^[3]

A média gyakran kiérdemli a jogos kritikát, de nem normális, ahogyan Donald Trump a klasszikus médiával bánik. Egyáltalán, manapság már csak kevés dolog tűnik normálisnak: nem

normálisak az új nagyhatalmi törekvések és a nukleáris fegyverkezési verseny, nem normális, ahogyan demokratikusan megválasztott elnökök hatalmát rendeletekkel és szükségállapot elrendelésével felülírják – és a nemzetek közti kommunikáció hangneme sem az.

Normális és magától értetődő egykor Európa összetartása volt. A megbízható nemzetközi partnerségek. A békeosztalék. A jólétünk, és annak globális növekedési opciói. Nem pedig az, hogy kereskedelmi háborúk vagy a világrend átalakításának Damoklész-kardja függ a fejünk felett.

2014 óta a normalitáson repedések jelentek meg. Moszkva a nemzetközi jog felrúgásával annektálja a Krímet. Kelet-Ukrajnában fegyveres konfliktus tör ki, amelyet a biztonságpolitikusok nem láttak előre, és nem ismerik fel benne az Európai Unió súlyos válságát. Németország néhány hónap alatt több mint egymillió menekültet fogad be. Kelet-európai EU-tagok „illiberális demokráciáknak” nyilvánítják magukat. Aztán 2016-ban következik két eddigi csúcspont: a Brexit, ami a közvéleménykutató intézetek ellenkező előjelű prognózisai miatt a többséget teljes meglepetésként éri, valamint az ingatlanmilliárdos Trump megválasztása az Egyesült Államok 45. elnökévé. Az utóbbi fejlemény annyira abnormális, hogy még maga Donald Trump sem számolt saját választási győzelmével. Azóta a béke nemzetközi rendjét, a biztonságot, a jólétet és a demokratikus értékeket is heves támadások érik, ahogyan a világgal való kapcsolatainkat is. Ez nemcsak az államközi kapcsolatokra, hanem a mi egymással való és egymás közti kapcsolatainkra is értendő, pontosan a

sikeres együttélésünkre a társadalomban, amit ez az utópia fejez ki: *ut omnes unum sint* – hogy mindnyájan egyek legyünk.

A világ abnormális lett, amit mi, akik még tudjuk, milyen érzés az, hogy valami „normális”, egzisztenciális veszteségként élünk meg. A normalitás elvesztét tapasztaljuk. A megszokott rend felbomlik, és egy disszociációs helyzetben, az „itt és most”-tól elidegenülten találjuk magunkat. A szociológusok ezt a jelenséget esetlegességnek nevezik. Sodródunk az adatok, információk és a naponta megjelenő nóvumok áradatában, és nem találunk többé stabil fogódzót.

Az új normális: a felbomló társadalom. Kétségkívül része van ebben az uralkodó relativizmusnak és egy olyan tudomány-, illetve politikafelfogásnak, amely nélkülöz mindenféle esztétikai, vallási vagy etikai visszacsatolást, ám az online felületek végezték el a munka oroszlánrészét, beteljesítve a maguk szerepét az újfajta válságok során. Lassan mutatkoznak már a technikai következmények, és még a technika legprominensebb apostolait is gondolkodóba ejtik. Régen szertefoszlott a lelkesedés az iránt az utópia iránt, hogy az online platformok a demokráciából még több demokráciát hozhatnak létre.

Amikor a kapitalizmus demokráciának látszik

Éppen Edward Snowden hívta fel a figyelmünket arra, hogy a közösségi médiák imidzse, amit kapitalista online platformok teremtettek maguknak, „a legsikeresebb megtévesztés azóta, hogy az [amerikai] hadügyminisztériumot átnevezték védelmi

minisztériummá”^[4]. Jóllehet utalása arra vonatkozik, hogy az állampolgárokat magántulajdonú technológiai gigászok tartják megfigyelés alatt, Snowdennek akkor is igaza volna, ha a techno-óriásoknak azt róná fel, hogy fejük tetejére állítják az olyan fogalmakat, mint „közösségi” és „médiák”. A fogalmak összevarása, a megtévesztés és a dezinformáció alkotja a központi magvát annak a digitális információs térnek, amely a weboldalak, közösségi médiák, blogok, keresőmotorok, azonnali hírszolgáltatók és e-mailek – röviden az online platformok – mellett ezek adattárolóit és szoftveralkalmazásait is tartalmazza.

Az online platformokat egyetlen dolog érdekli: a teljes kommercializáció. Már a közösségi médiák sem mások, mint reklámfelületek. A Facebook esetében egy-egy felhasználó kb. 232 amerikai dollárt ér – ha a cég 464 milliárd dollárra becsült értékét (2019. február) elosztjuk a mintegy két milliárd aktív felhasználó számával.^[5] Ezt a pénzt valahogy ki kell gazdálkodni, mert felhasználói, mint ismeretes, térítésmentesen használják a Facebookot. Ezért aztán Mark Zuckerberg mindent elragad tőlünk, amit a Facebookon posztolunk – mint ingyenes tartalmat digitális hirdetési tere számára, majd csengő pénztermékre váltja be a hirdetőknél és reklámügynökségeknél. Ha már mi nem tesszük, akkor végül is egy harmadik félnek kell viselnie a hirdetési platform fejlesztésének és meglehetősen drága működtetésének költségeit. A mi tartalmunk, a négyéves kisfiú fotója és a King Charles spánielről készült pillanatfelvétel között (gyerekek és állatok mindig menők) aztán a legújabb várositerepjáró-

modellt hirdetik, lehetőleg álcázva, pseudo-zsurnalisztikus találásban.

Aki az információs térben szörfözik, azt szünet nélkül ellenőrzik. Amilyen webhelyen időzik egy ember, amelyikhez visszatér, arra irányul a figyelme – gondolják a digitális ellenőrök, amelyek közé egyaránt tartoznak vállalatok és kormányok. Ez a figyelem pénzt ér. Aki repülőjáratot keres a neten, annak szállodára is szüksége lehet, ahová utazik, ott el akarhat látogatni egy rendezvényre, vagy érdekelhetik a vendéglők. Ezért aztán kereskednek a figyelemmel, valahogy úgy, mint egy tőzsdén.

Az online platformok saját, cégen belüli börzeegységeket fejlesztettek ki, regisztrálják, ami iránt a felhasználó érdeklődik, és árcédulával látják el. Ezt a csomagot vállalatok saját börzéin megvételre ajánlják fel, illetve árverezik. Aki kész leróni egy „érdeklődés” árát a platform működtetőjének – az ilyenek hirdetési ügynökségek és vállalkozások, amelyek hirdetési büdzsét nyitottak a Facebooknak, a Twitternek vagy a Google-nak –, továbbdolgozhat vele, és reklám-e-maileket küldhet a felhasználók postafiókjába.^[6]

A mechanizmus, amelynek segítségével a felhasználó érdeklődésére összpontosítanak, nem teszi lehetővé, hogy az online platformok vagy hirdető-ügyfeleik valami egyebet kínáljanak, mint azt, ami megfelel a felhasználó érdeklődésének. Annak a legbiztosabb lehetősége, hogy pénzt kereshetnek, csak akkor áll fenn, ha a felhasználó érdeklődését sikerül hajszálpontosan kielégíteni. Olyan információt, amely egyáltalán nem tartozik az érdeklődési körébe, még csak el sem juttatnak hozzá. A

felhasználó önreferenciáinak nyomatékosítása és saját érzékelésének erősítése rendszerszerű, és központi része a digitális platformok üzleti modelljének, amelyeknek most, amikor mindinkább hatósági szabályoknak és fogyasztóvédelmi követelményeknek kell megfelelniük, nehezükre esik, hogy utólag korrigálják a problémákat, amelyek igen mélyen gyökereznek üzleti modelljeikben.

Míg az online platformok a 21. század reklámkatalógusai, mi, felhasználók egyszerűen megbolondultunk:^[7] azt hisszük, hogy épp a profitorientált globális konszern platformjai a vélemény szabadság és a politikai akaratképzés megfelelő fórumai. ^[8] Ezért van az, hogy a kereskedelmi online platformokon megjelenő tények, érdekek és eszmék saját politikai meggyőződésünké is váltak. Ezeken a helyeken minden átpolitizálódik: Futball Ófelsége, a táplálkozásunk, a tőkepiacok. Aki nem vegetáriánus módon táplálkozik, a klíma kártevője lesz, akárcsak azok, akik repülővel mennek nyaralni; aki keveset mozog, az az egészségügyet károsítja... Hogyan bánjanak a labdarúgó-egyesületek a jobboldali populista szurkolókkal a stadionban és stadionon kívül? Hogyan viszonyuljanak a pénzpiac szereplői a tőzsdei árfolyamokhoz, amikor a piacok minden eddiginél élénkebben reagálnak a politikára?

A normalitás elveszte tehát az olyan bonyolult belső folyamatokra is kiterjed, amilyen a politikai véleményalkotásunk. Ez utóbbi már nem úgy működik, mint ahogyan azt a Német Szövetségi Köztársaság alkotmányának kidolgozói, még a 20. században, elképzelték: „A pártok közreműködnek a nép politikai

véleményalkotásában.”^[9] Együttműködnek, hát persze, de már nem ugyanazzal a súllyal és nem ugyanabból a monopolisztikus pozícióból, mint korábban. A pártokat többé a nemzeti határok sem védik meg az külső behatásoktól. Nemzetközi szereplők szereznek befolyást nemzeti véleményekre anélkül, hogy akár betennék a lábukat idegen államok területére.

Aki bizalmatlanságot vet, változást arat

Washington, délután fél négy, 2016. október 7-e, péntek. Az amerikai elnökválasztási küzdelem a Donald Trumpgal szemben álló Hillary Clintonra éleződött ki. A választás napjáig már csak néhány hét van hátra, amikor a Fehér Ház azon a péntek délutánon arról tájékoztatja az amerikai népet, hogy Oroszország tevőlegesen beavatkozik az amerikai választási küzdelembe.

„Az Egyesült Államok hírszerző ügynökségeinek meggyőződése, hogy a nemrég történt, jogosulatlan behatolást az amerikai polgárok és intézmények e-mailjeibe az orosz kormány rendelte el. A lopásokat azért követték el, a tartalmakat pedig azért hozták nyilvánosságra, hogy ezáltal megzavarják az amerikai választási küzdelmet. Ilyenfajta tevékenységekre csak a legfelsőbb orosz kormánykörök adhattak felhatalmazást.”^[10]

A riasztó kormányközlemény hatása kérészéletű. Egy órával később, mintegy a Fehér Ház figyelmeztetésének igazolásaként, a WikiLeaks több mint 20 ezer oldalnyi e-mail-váltást hoz nyil-

vánosságra, amit orosz hekkerek John Podestától, Hillary Clinton választási kampányfőnökétől loptak el. Az anyagok mély betekintést engednek Hillary Clinton választási kampánymunkájába. Felfedik a Clinton Alapítvány munkáját és érdekkonfliktusait, a demokrata választási kampánystratégiát, Hillary Clinton Wall Street-i szponzorainak adatait, akiket szinte gyöngéden körbe udvarol, továbbá munkatársaival kapcsolatos pletykálkodását. Az amerikai biztonsági hatóságok egyik vizsgálata később kiderítette, hogy Hillary Clinton nyilvánosságra hozott e-mailjeinek hitelességéhez nem fér kétség.^[11]

Ezt a Clinton-kampány egyik szóvivője eleinte nem hajlandó elismerni: „Nem fogjuk igazolni, hogy a lopott dokumentumok, amelyeket Julian Assange [a Wikileaks alapítója], aki nem rejti véka alá, hogy kárt akar okozni Hillary Clintonnak, valódiak.”

A nyilatkozat középpontjában álló fogalom a „kárt okozni”. Aki egy uralkodó gazdasági, illetve kormányzati berendezkedésnek vagy tekintélynek kárt okoz,^[12] vagy az a szándéka, hogy „azt akarata ellenére bizonyos cselekményekre kényszerítse”, felforgató magatartást tanúsít.^[13] Ezért is hangzik úgy a vád, amelyet Robert Mueller különleges ügyész 2018 februárjában 13 orosz állampolgár ellen emel, hogy az illetőknek kinyilvánított céljuk volt „bizalmatlanságot kelteni [amerikai] elnökjelöltekkel és általában a politikai rendszerrel szemben”^[14]. Oroszország célja, mint ezt a nemzetbiztonsági hatóságok vezetői, John Brennan (CIA), James Comey (FBI), James Clapper (DNI) és Michael Rogers (NSA) 2017 januárjában a még kormányzó Obama-adminisztráció számára egy részben titkos jelentésben

összefoglalják, az volt, hogy „aláássa az Egyesült Államok demokratikus működésébe vetett közbizalmat, megrágalmazza Clinton miniszterasszonyt, továbbá károsítsa választhatóságához fűződő jogait és rontsa elnökké választásának esélyeit.”^[15]

A felforgatás – „bizalmatlanság [és] paranoia” keltése egy kormány ellen^[16] – karrierje több mint kétszáz éve kezdődött. Először a 18. század végén, a nagy amerikai és franciaországi forradalmakkal kapcsolatban jelent meg. A kontinentális Európában – Franciaországban, Németországban és Olaszországban – a „felforgatás”, „felforgató” szavak használatuk gyakorisága alapján csak a II. világháború végétől kezdve tettek szert egyre nagyobb jelentőségre. Németországban napjaikban jutottak a csúcusra.^[17]

Mindazonáltal pontosítanunk kell: amikor itt felforgatásról beszélünk, a szó eredeti értelmére gondolunk, a felforgatásra mint olyan tevékenységre, amely a fennálló uralmi rend megdöntésére irányul. Enyhébb formában az a célja, hogy valószínűbbé tegye a népesség ellenállását a fennálló renddel szemben.^[18] Ennek érdekében a szubverzió mindig a szívet és az értelmet – *hearts and minds* – veszi célba. Magát az áldozatot teszi fegyverré, mihelyt az – akár erőszakos, akár erőszakmentes módon – saját rezsimje ellen fordítja intellektuális erejét.

Vajon a technológiai haladás névtelen erői is kifejthetnek felforgató hatást? Hiszen a digitális átalakulás mindeddig példátlan technikai lehetőségei a rend ellen irányuló, könnyen berobbanó erőt fejtenek ki. Theodore Rooseveltnél már az első ipari forradalom idején is aggódva tette fel a kérdést, hogy vajon hány

politikai fordulat, mennyi pusztítás kiindulópontja lesz a technikai haladás: „Valamennyien feszülten kémleljük a jövőt, és megpróbáljuk megjósolni a hatalmas ipari forradalom által felszabadított vak erők hatását. Egyelőre nem tudjuk, mit tartsunk a nagy népvándorlásokról, a városok kiterjedésének megnövekedéséről, a tömegek nyugtalanságáról és elégedetlenségéről, és azoknak a rossz érzéséről, akik a jelenlegi rend támogatásának szentelték magukat.”^[19] Ma is ugyanolyan helytálló ez a mondat, mint annak idején volt.

Még ha a felforgatás fogalma a fordulattal, a forradalommal és a lakosság erőszakos aktivitásával összefüggésében bukkan is fel, azért a politikában a szubverzív cselekvés nagyon eltérő következményekkel járhat. A szubverziónak – a hidegháború idejével és az amerikai választásokba való orosz beleavatkozással ellentétben – nem kell feltétlenül államközi indíttatásúnak lennie. Államon belüli szereplők külső motiváció nélkül is folytathatnak felforgató tevékenységet.

Fordulatot célzó tevékenységként a felforgatás szabadelvű társadalmak alkotmányos rendszerén belül rendszerint csak akkor megengedett, amikor már nem lehet megbízni a demokratikus, parlamentáris és jogállami struktúrákban. Ha a visszásokokat másként már nem lehetséges orvosolni, akkor a polgároknak szabad igénybe venniük az állampuccs eszközét, hogy ne egyszerűen kormányváltást, hanem egyszersmind hatalomforma-váltást is előidézzenek. Ezért engedélyezi a Német Szövetségi Köztársaság alkotmánya 20. cikkelyének 4. bekezdése

vészhelyzetben – ellenállás esetében – a magánerőszak alkalmazását.

Aki ezzel szemben a felforgatást mindössze a fennálló politikai viszonyok elleni lázadás erőszakmentes aktusaként fogja fel, azt mondja, hogy egy szabadelvű és demokratikus állam a felforgatásból még profitálhat is, ha az hozzájárul regenerálódásához, szükséges megújulásához, sőt akár a fennmaradásához is.

Az erőszakmentes szubverzió akkor válik általánossá, ha a lakosság fegyvertelenül tiltakozik. Erőszakmentesen és jogszerűen zajlott például a Hambachi-erdő fáinak 2012-ig tartó „elfoglalása”. A nép részéről gyakorlatilag erőszakmentesek voltak a lipcsei Szent Miklós-templomban 1989-ben tartott békeimák, amelyek a Német Demokratikus Köztársaság bukásához vezettek. Még azok a tengeri mentők is szubverzív módon járnak el, akik a Földközi-tengeren megmentik az afrikai menekülteket a vízbefúlástól, ugyanis teljesítik azt a feladatukat, hogy a tengeren veszélybe kerülteket segítsék, ugyanakkor azonban nyomást fejtenek ki ezzel az Európai Unióra is, hogy nézzen szembe a menekült-problematikával, és találjon megoldásokat. Ha a felforgatás ilyen értelemben erőszakmentes, és pusztán a politikai befolyásolás szándékával zajlik, jól illeszkedhet a hibrid módszerek közé.

Államközi szinten a dolgok állása egyébként is egyszerűbb: ha egy ellenséges állam befolyásolni akarja egy másik államban a politikai akaratot, nem igazán tehet egyebet, mint hogy a felforgatás eszközéhez folyamodjon, mert a politikaváltás általános folyamataira nincsen befolyása. Ennek alternatívájaként

csak erőszakot alkalmazhat, a másik állam környezeti intelligenciája elleni súlyos támadásoktól kezdve egészen a katonai erő alkalmazásáig.

Hazugsággal a sikerhez

A média kezdettől fogva fontos szerepet játszott a felforgatás, illetve a valóság értelmezésének felségjoga szempontjából. Az I. világháború kitörésekor a hangfelvétel számított a legújabb technológiának. II. Vilmos császártól röviddel a háború kitörése után rögzítették e mondatot: „A béke kellős közepén megtámad bennünket az ellenség. Fegyvert kell hát ragadnunk: minden ingadozás, minden habozás a haza elárulása volna.”^[20] Már akkor, pedig a háború még csak néhány napja tartott, elkezdtek alternatív tényekkel operálni, valójában ugyanis Németország volt az, aki északnyugat felől támadást indított Franciaország ellen, s ennek során megsértette Belgium és Luxemburg szuverenitását. A II. világháborúban következett a rádiókészülék, ami a Harmadik Birodalomban nemzetiszocialista propagandát terjesztett, aztán a televízió.

Ma a digitális információs tér az, ahol a politikai értelmezés felségjogáért folyó harcokat vívják. „A hálózatok játszották a kulcsszerepet abban, ami 2016-ban az amerikai politikában történt”, véli Niall Ferguson történész, az angolszász világ elismert szakérője.^[21] Ez kifejezetten magában foglalja az online hálózatokat is. Donald Trump választási vezérkarának a Facebook, a

Twitter és a Breitbart segítségével sikerült olyan, széles néprétegeket átfogó hálózatot kiépítenie, amelynek közvetítésével jeltöltjük üzenetei közvetlenül és minden további beavatkozás nélkül jutottak el pontosan azokhoz az emberekhez, akik szívesen elhitték azokat a választási üzeneteket, amelyek Amerika bajairól és kétségbeeséséről, korrupt politikai elitekről vagy a fokozódó kriminalitásról szóltak. Donald Trump ezt egyetlen rövid tweetben foglalta össze: „A tweetek nélkül nem lennék itt.”^[22] Donald Trump, a Twitter-elnök... A Twitter nélkül soha nem jutott volna idáig.

Ahol a katonai erőszak alkalmazása a háttérbe húzódik, vagy még csak szóba sem jön, a felforgatás és a hibrid támadások nagy mértékben kénytelenek az információs tér hatalmára támaszkodni. A lényeg, hogy ellehetetlenítsék a tényeket, a nyilvános diskurzusba vetett bizalmat, a politikai helyzet szabad és ésszerű értékelését, valamint a konszenzusteremtést. Ezek helyére lépnek az alternatív tények, az érzelmi befolyásolás és a provokáció, hogy kételyt, bizalmatlanságot szítsanak és megosszák a társadalmat.

Az is egy hazugság volt, ami 2017 tavaszán váratlanul komoly konfliktust robbantott ki úgyszólván a semmiből Katar és Szaúdi-Arábia között. Noha Katar védelmi uniót alkotott a szunnita szaúdiakkal és az Öböl-régióban az USA legnagyobb támaszpontjául szolgált,^[23] a két ország között olyan viszály robbant ki, amely csaknem katonai összecsapássá eszkalálódott, mégpedig egy olyan térségben, amely amúgy is puskaporos hordónak számít.

Minden egy ismert és bevált módon végrehajtott digitális támadással kezdődött. 2017 áprilisában hekkerek megtámadták a katari állami hírügynökség, a Quatar News Agency (QNA) kevésbé biztonságos webhelyét, és azonosítottak egy sebezhető pontot az ügynökség hálózatában. A hekkerek néhány napon belül e-mail-címekre, jelszavakra és hírekre tették rá a kezüket. Végül 2017. május 23-án 12 óra 13 perckor, az interneten, jóllehet nem közvetlenül, de a világ nyilvánossága elé léptek.^[24] Rendkívül veszélyes politikai tartalmakat adtak a katari kormány szájába. A katari emír, hangzott a hazug üzenet, a síiták által kormányzott Iránt, Donald Trump fő ellenségét, iszlám hatalomként méltatta. Az üzenet emellett „a palesztin nép törvényes képviselőjének”^[25] nevezte a Gázai övezetben Irán által támogatott Hamaszt, amelyen belül egyre több szunnita állt át a síitákhoz.

A QNA pánikba esve azonnal lekapcsolta webhelyét, és több órára elérhetetlenné vált; közben a katari emír láthatólag nagyon igyekezett elmagyarázni, hogy ezeket az álhíreket (*fake news*) másvalaki adta a szájába. Nem sokra ment vele, Szaúdi-Arábia közbenjárására a mindössze körülbelül kétmilliós lakosságú ország rövid időn belül elszigetelődött. Azzal a váddal, hogy Katar támogatja a terrorizmust a térségben, Szaúdi-Arábia, az Egyesült Arab Emírátusok, Egyiptom és Bahrein katari állampolgárokat utasított ki, és elzárta a Perzsa-öböl mellett fekvő kis államba vezető tranzit-útvonalakat.

Az, hogy egy digitálisan magas fokon hálózatosított társadalom viselkedése egyre kevésbé megjósolható, a hálózatiság lényegéhez tartozó jellegzetesség. Ez az egyik dolog. A rendszerte-

oretikusokban azonban felvetődik egy másik kérdés is: miféle dinamikát idéz elő a külpolitikában a digitalizáció? Vajon milyen arányban játszik szerepet korunk politikai válságaiban a digitális információs tér és az online kommunikáció?

„Új dolog, hogy az államok, kormányok de egyes polgárok vagy éppen intézmények befolyásolásának módszerei is hihetetlen módon megsokasodtak”, fejt ki továbbá Wolfgang Ischinger, a digitális platformoknak mint a felforgatás nagy horderejű eszközeinek a potenciálját is szem előtt tartva. „Ma már nincs szükség arra, hogy egy kormány elküldjön valakit, aki azonosíthatóan közzétesz egy újságcikket, vagy ledob egy rölapot. Ma olyan eljárásokkal, mint a trollkodás – tucatjával, ezrével, száz-ezrével mozognak emberek a közösségi médiákban, akik próbálnak hangot adni bizonyos véleményeknek –, elő tudnak mozdítani egy formális gazdasági szankciók vagy erőszakos katonai lépések szintje alatti hibrid cselekvésmódot.”^[26]

Az új kommunikációs formák őrvénye régóta beszippantotta a klasszikus médiát is. Egyre több hírfogyasztót veszítenek a közösségi hálózatok javára, és maguk is kezelnek digitális platformokat, azt remélve, hogy feltartóztathatják egyre gyorsabb hanyatlásukat.

Politikacsináló narratívák

Alkalmas vajon a digitális információs tér dinamikája a 21. század csatáira, amelyeket nem csak katonai erővel, hanem „geril-

la-információsháborúként” is vívnak, miközben elmosódik a há-
tár hadviselők és civilek között? Herbert Marshall McLuhan mé-
diateoretikus már vagy ötven évvel ezelőtt elgondolkodott ezen.
[27]

Néhány kormány, de nem állami szereplő is réges-régen egy-
értelmű igennel felelt magában erre a kérdésre. Megértették,
hogy a 21. században a háborúk multimodálisak, több dimenzi-
óval rendelkeznek, és nemcsak a fizikai csatatéren, hanem az
információs térben is vívják őket. Történeteket mesélnek és nar-
ratívákat terjesztenek, hogy érzelmileg megérintsék az embere-
ket, s hogy biztosítsák maguknak a támogatásukat. Ugyanakkor
a német egyetemeken régóta divatba jött a digitális történetme-
sélés, a *digital storytelling*, mert a bonyolult technikai folyama-
tok is könnyebben érthetővé válnak, ha egy jó sztoriba csoma-
golják őket.

A digitális információs tér legelkötelezettebb szereplői közé
tartozik a muszlim világ. Immár évek óta olyan professzionális
módon használják, hogy az európaiak csak ámulhatnak. Miköz-
ben mi beérjük annyival, hogy a WhatsApp-csoportban meg-
szervezzük a következő gyerek-születésnapot, esetleg leveseket
vagy lakkozott körmöket ábrázoló fotókat posztolunk az Instag-
ramon, más országokban a legnagyobb mértékben átpolitizált
közeggé lett az információs tér. Minden csatornán, mindenféle
elképzelhető narratívával, képekkel, fenyegetésekkel és orbitá-
lis hazugságokig terjedő csábításokkal ontják az online prédiká-
ciót, az indoktrinációt és a politikai agitációt, s még attól sem ri-
adnak vissza, hogy terrorszervezetek számára utánpótlást tobo-

rozzanak. Azokban az államokban, amelyek már évtizedek óta újra és újra erőszakos katonai konfliktusokkal szembesülnek, úgy tűnik, jóval erősebben kialakult annak tudata, hogy az információs tér felhasználható célzott stratégiai információs kampányok folytatására, mint azokban az országokban, amelyekben béke uralkodik. Ez azonban épp most változik.

Mindössze néhány nappal a 2019. májusi Európa-parlamenti választások előtt a Rezo nevű YouTuber közzétett egy *Így teszik tönkre a CDU-t* című videót. Videója, amely a német néppárt pozícióit támadja, 14,5 millió kattintással átütő siker lett. Nemcsak a klip széleskörű visszhangján, hanem a CDU reakcióin is érdemes elgondolkodni. A megtámadottak első reakciója a lefitymálás és a megrendszabályozással való fenyegetődzés. A videó hangulatkeltés, járta pártkörökben. Azonban a pártok, a német szövetségi kormány még nem fogta fel, hogyan működik manapság a kommunikáció. Még nem fedezték fel maguknak az információs teret a hatásos kampányok közegeként. Az ilyen kampányokat meg kell tervezni, előzetesen tesztelni, aztán a startjel megadása után menedzselni. Semmit sem bízunk a véletlenre. A *policy maker*, a politikacsináló ugyanis, tekintet nélkül arra, hogy állami szereplő-e, vagy sem, aktívan alakítani akarja a politikai üzenetekről folyó diszkurzust, és irányítani akarja a lakosság befolyásolását. A védelmi tanácsadók ma már a *lájkok*ért folyó háborúról beszélnek.^[28] Aki ismeri a narratíváját, előre elkészíthet tartalmakat, és készenlétben tarthatja őket a fiókban az információs térben folyó legközelebbi online kampányhoz. Az ilyen tartalmak közé tartoznak a jelszavak, tevékenységek-

hez kapcsolódó címek és alcímek, ígék, amelyek egy-egy politikai vagy katonai cselekvést különösen találóan írnak le, infografikák, posztterek, videók, sőt még statisztikák is a kommunikálandó tények alátámasztására – csupa online műalkotás, amelyekre könnyű rákattintani, s amelyeket ugyanilyen könnyű megosztani is. A kommunikáció súlypontja ennek során egy-egy politikai üzenet vizualizálása, hisz az emberek már nem sokat olvasnak.

Az információs térben folytatott politikai kommunikáció célja tehát elsősorban adatok előkészítése a kívánt politikai üzenet megtámogatására. A diskurzushoz nyers adatokat gyűjtenek, és „kipreparálják” a kívánt narratívát, amit azután posztolnak. Ezután hozzák meg ítéletüket a felhasználók. Döntenek szimpátiáikról, arról, hogy támogatják-e a posztolt véleményt, vagy pedig az ellenkező álláspontra helyezkednek. De nemcsak a kiválasztott képek és szövegek váltanak ki érzelmeket, hanem maga a csatorna is.

A közösségi médiák közvetítésével az üzenetek személyesebbeknek hatnak. Közvetlenebbeknek, hitelesebbeknek tűnnek – mint Donald Trump tweetjei. Az üzenet széleskörű hatásossága azon is múlik, hogy a politikai szereplők rendeltetésszerűen használják-e az online platformokat.

A Twitter esetében a hírek gyorsan, széles körben terjednek, és mivel a hitelesség benyomását keltik, könnyen mobilizálják a felhasználókat. A lehetőleg konzisztens tartalmak terjesztésében nagy segítséget jelentenek a hashtagek; megkönnyítik a hasonló tartalmak keresését.

A Twittertől eltérően a YouTube egy-egy narratíva vizualizációját könnyíti meg, s így fokozott mértékben mozgatja meg a publikum érzelmeit. A YouTube kitűnően megfelel oktatási csatornának is, és használják is erre, a sminkiskoláktól a szélsőséges tanokat terjesztő vallási iskolákig.

Az Instagram vagy a Pinterest ezzel szemben egy-egy narratívával kapcsolatos, állóképekből készített vizuális montázsok megjelentését teszi lehetővé; ugyanúgy, mint a Twitteren, ezen a platformon is kereshetünk és találhatunk hasonló tartalmakat.

Ha valaki hasonló gondolkodásúakkal akar bezárkózni egy visszhangkamrába, a Facebookon a lehető legjobb helyen van. Az emberek nemcsak egy narratíva számos különböző formátumait posztolhatják, a platform nagyfokú ismertsége folytán növekednek az esélyek, hogy a hagyományos média is igénybe veszi. Egy Facebook-bejegyzés jelentheti a televízióba vagy a nyomtatott médiába való „átugrás” lehetőségét.

A digitális információs térben folytatott célzott kommunikáció tehát nem mellékes dolog, hanem tervezést, költségvetést és személyi állományt tesz szükségessé. Az anyagi ráfordítás azonban még a nem állami politikai szereplőket sem rettentí el. A Hezbollah egy körülbelül 30 munkatársból állandó csapatot tart fenn kizárólag internetes kommunikációhoz, olyan mintát szolgáltatva az Iszlám Államnak, amely – mivel az interneten igen sikeres – ifjúsági mozgalomként is megállja a helyét.

Olyanok számára, mint a németek, az online platformok gátlástalan használata politikai kampányok és a célzott kommuni-

káció céljára egyenesen frivolnak, sőt akár veszedelmesnek tűnik. A német történelem legsötétebb óráiban ugyanis szintén narratívák voltak, amikkel tudatosan kialakítottak a lakosságban egy bizonyos véleményt. Ezek sorába tartoztak az olyan üzenetek, mint a „Hitler Németországról” kampány az 1932-es választások alkalmával, „a hosszú kések éjszakája” elnevezés a Röhm-puccs idején, vagy a szöveg az „antifasiszta védőfalról”, amely az NDK-t volt hivatva megvédeni a korábbi náciktól. Az NDK kormányzatának narratívája így szólt: az NDK-ban nincsenek nemzetiszocialisták – valamennyien nyugaton telepedtek le. Ezt a történészek ma másként tudják. A tegnap narratívái ennek ellenére még ma is ugyanúgy működnek.

A médiajelenlét költségei

Az, hogy az információs műveletek számos politikai szereplő körében igen kedveltek, annak is tulajdonítható, hogy az információstér-használatnak viszonylag alacsony az alapköltsége. A digitális platformok használata térítésmentes, a hirdetőik szponzorálják. Akinek szándéka, hogy némi pénzt fektessen be és célzottan megszólítson bizonyos társadalmi csoportokat, eljárhat úgy, mint a Republikánus Nemzeti Bizottság (RNC) a 2016-os amerikai elnökválasztási küzdelem során. A demokrata Barack Obamától inspirálva, aki 2012-es választási kampánya alatt először foglalkoztatott egy matematikusokból, fizikusokból és adat-elemzőkből álló csapatot, hogy a választók Facebook-adatait kiértékelve személyre szabott üzenettel célozzanak meg minden

egyes bizonytalant, az RNC több mint 175 millió dollárt fektetett az amerikai Internet-felhasználók kielemezésébe.^[29] Mindent megtudtak a választókról, akik bizonyosan vagy még nem egészen bizonyosan Donald Trump mellett készültek dönteni. A párt tudta, melyik sörfajtát isszák a legszívesebben, milyen állapotban van az autójuk, tudta, mennyi idősek a gyerekeik, és milyen iskolákba járnak, hogy mennyi hitelt vettek fel és milyen lejáratra, hogy milyen cigarettát szívnak, tudta, ha valakinek fegyvertartási engedélye van, és ismerte az olvasmányait is.^[30] Ezen a módon, és a Cambridge Analytica, egy kétes hírű, egykori brit adatelemző cég közreműködésével és az illetők személyiségi jogait megsértve, számítástechnikai úton 220 millió amerikai választó profilját dolgozták ki.^[31] Semmi sem maradt titokban, és csak megfelelő módon kellett megszólítani őket, hogy szavazatukat a „helyes” jelöltnek adják.

A szubverzív támadó számára előnyt jelent, hogy az információs tér alacsony alapköltségei miatt mindenféle információs műveletet könnyű végrehajtani, ugyanakkor azonban hátrányt is. Ugyanis üzenetének címzettjei is könnyen és jóformán akadálytalanul mozoghatnak az információs térben. Mobilisak, és a mobilitás gyorsan eltereli az ember figyelmét egy információs műveletről. Ezért aztán nehezen ellenőrizhető, hogy a felforgató célú online ráhatások valójában hogy jönnek be. Hogy vajon mennyire megbízható az információs tér segítségével alkalmazott indoktrináció? Erre a kérdésre – gondterhelt pillantást vetve a legfrissebb társadalmi fejleményekre és az embereknek a politika részéről való elhanyagolására – szívesen mondanánk

azt, hogy „nagyon megbízható”. Tényleg az amerikai választási küzdelembe történő orosz beavatkozás alapozta meg Donald Trump megválasztását? Aligha bizonyítható. Amint a tömeges adatok algoritmikus kiértékelésére általában áll: felismerhető a korreláció, ez esetben az orosz cselekvés és az amerikai választások kimenetele között, de bizonyított oksági lánc nem építhető fel.

Cenzúra az interneten

„Az információs tér lehetőségek sokaságát biztosítja olyan aszimmetrikus intézkedések számára, amelyek csökkentik az ellenség harckészségét”, írja Valerij Geraszimov orosz tábornok már 2013-ban, az arab tavaszról szóló, nagy visszhangot keltett esszéjében.^[32] Az orosz fegyveres erők megértették, hogy egy olyan társadalom mélységi penetrációjának, amelynek központi idegrendszere az internetes adat- és információ-átvitel, van egy nagy gyengéje. Az információs teret nem csak hekkerek kémlelik és okoznak benne károkat, amikor az információt fegyverré alakítják át – mint ezt a 2016-os amerikai elnökválasztási küzdelem is látványosan illusztrálta –, vagy kártékony programokat telepítenek. Ott, ahol az információs tér a hír- és véleménycsere piaca gyanánt minden felhasználó előtt nyitva áll, az állam pedig alig cenzúrázza, bárki terjeszthet szándékosan és stratégiai céllal kifinomult üzeneteket és folytathat felforgató tevékenysé-

get, hogy az ellenfelet lélektanilag befolyásolja és egy bizonyos magatartásra készítse.

Ennek során az információs tér egy sajátos működési jellegzetességét használják ki: a visszajelzést, a *feedbacket*. S van-e köztünk olyan, aki nem szokta meg réges-rég a mindennapos *feedbacket*? A Facebook-lájkokat, az online kommenteket, a megosztást, a *retweetet*, sőt a folyamatos munkahelyi visszajelzést, amelyet egyes vállalati tanácsadók a napi ügymenet valós idejű intézményévé akarnak tenni? A *feedback* az embernek arra a vágyára játszik rá, hogy mindig mások vigyenek értelmet és örömet az életébe.

E vágy beteljesülését végül is – gondolták a technológia emberei a 2000-es években – át lehetne helyezni az információs térbe, ami így soha nem volt hatótávolságra tenne szert, mert más emberek ezrei, sőt milliói válhatnának barátokká és követőkké. A *feedback* mindazonáltal kivált egy komolyan veendő hatást: zárja a kibernetikus szabályzókört. Az ember ugyanis egyszerre egy zárt kontrollhurokban találja magát, megfigyelik, ellenőrzik, egyszersmind pedig vezérelhetővé is válik. Tesz valamit, kap egy visszajelzést, aztán ismét tesz valamit – ugyanazt vagy másvalamit, csak hogy új visszajelzést kapjon.

Mivel az emberi psziché manipulációja nem ismerhető fel egykönnyen, a befolyásolás áldozata valószínűleg ritkán veszi a fáradságot, hogy kinyomozza, elkapja a digitális térben a felforgató cselekmények előidézőjét, vagy hogy akár védekezni kezdjen. Pontosan ez a véleménye Valerij Geraszimovnak: a 21. században egy idegen kormány szubverzív magatartása több le-

hetőséggel, mint kockázattal jár. Politikai célokat lehet elérni anélkül, hogy katonai eszközökhöz kellene nyúlni. Ahelyett, hogy az ellenféllel szemben katonai kényszert alkalmaznának, azt kell elérni, hogy a másik kulturális fölénye, az iránta táplált pozitív érzelmek, illetve az érvek győzzék meg.

Napjainkban éppen a fejlett, demokratikus, szabad piacgazdasággal rendelkező társadalmakkal szemben hajthatók végre az információs műveletek minden eddiginél hatékonyabban. A demokratikus berendezkedésű államok esetében, ahol törvények garantálják a vélemény- és szólásszabadságot, épp nyitottságuk fordulhat önmaguk ellen, amikor az ideológiai ellenfél pont ezt a szabadságot használja ki az információs térben felforgató tervei megvalósításához. Könnyű szerrel kiadhatja magát valaki másnak, hogy ideológiákat és hazugságokat terjesszen, amelyek aztán szöveget ütnek az emberek fejében, és lassan hatni kezdenek.

Jóllehet számításba sem kell vennie, a támadó már jó előre megelőzi az áldozat „információs második csapását” azáltal, hogy a maga információs terét – s ebbe kifejezetten beletartozik az online kommunikáció – államilag ellenőrzi és cenzúrázza. Oroszország, Kína, Észak-Korea és Törökország csak a legközismertebb azon államok közül, amelyekben állami médiák, kormánybarát adók és újságok terjesztik a híreket, miközben az ellenzéki hangokat erőszakosan elfojtják. Oroszország még alternatív internetet is létrehozott, saját online infrastruktúrát, amelyre a Kreml egy nyugatról érkező biztonsági fenyegetés esetén egyetlen gombnyomással átkapcsolhat.^[33] Ez után az

orosz lakosság ugyan még mindig beléphet az internetre – de csak az orosz ellenőrzésű információs térben, „a Vörös Hálón”, a nemkívánatos nyugati információszolgáltatóktól elkülönítve és a demokratikusan irányított nemzetek, nevezetesen az Egyesült Államok befolyásától elzárva. A váltás az orosz internetre, amelyet Oroszország Kínának is a rendelkezésére bocsátana, ráadásul egy igen kívánatos mellékhatással is járna: az oroszok hekkertámadásai veszélytelenebbül végrehajthatókká válnának, mert egy másik (internet-)rendszerben kellene visszakövetni őket.

Az egyiptomi rezsim is tanult az arab tavaszról. Amikor a kormányzat ellenfelei 2011-ben a Twitter és a Facebook segítségével szerveződtek és gyülekeztek az utcákon, hogy Hoszni Mubarak ellen demonstráljanak, utóbbi a kormánya és az internet-szolgáltatók közti telekommunikációs szerződésekre hivatkozva gondoskodott arról, hogy Egyiptomban lekapcsolják az internetet. Azóta az információhoz való online hozzáférés tekintetében még sokkal rosszabb a helyzet. 2011-től a hatalom új egyiptomi birtokosai drasztikusan megszigorították az internet ellenőrzését. Manapság a szelektív szűrés helyett nem pusztán egyes webhelyek, hanem teljes nettartalmak blokkolása az általános.

Inger-reakció-játék

Azt az eredetileg gazdasági szándékot, hogy minden egyes internetfelhasználót egy bizonyos cselekvésre bírjanak, és szelíd nyomással megnyerjék az egészségesebb életmódnak, jobb au-

tózásnak vagy csak egyszerűen a több fogyasztásnak, a politikai szereplők a maguk számára már régen újradefiniálták a célból, hogy globális véleményeket befolyásoljanak és egész társadalmakat irányítsanak. Az információs tér azért jelent szilárd alapot ehhez, mert részletesen feljegyzi életünk adatait – azt, amit többségünk éppen keres, tesz, olvas, vásárol, végez, átél.

„Napjainkban az a cél, hogy megismerjük a tömegek általános törekvéseit. Így az ember totálisan uralható lesz”, állapítja meg igen helyesen Adrian Lobe publicista és politológus.^[34]

Egy állam vagy egy nem állami szereplő számára felvilágosítással szolgálhatnak az efféle trendleírások, végső soron azonban a következő lépés a lényeg: hogy vajon hogyan lehet kezdeményezni vagy befolyásolni a trendeket, és ezzel elérni az egész társadalmat?

Az internet kereskedelmi véleményformálóit nevezik befolyásolóknak, *influencerek*nek is – mert hallgat rájuk a YouTube, az Instagram és a Twitter számos felhasználója. A politikai térben is léteznek *influencerek*, s ma egy politikai – legyen bár külföldi – szereplőt semmi sem tart vissza attól, hogy ugyanazokat az eszközöket használja, mint a piacgazdasági orientációjú hirdetők. Ha azonban az emberek befolyásolása mégis finomabban zajlik, amikor dezinformálást, hazugságot és álcázást vetnek be (és van ugyan neve, mint a Guccifer 2.0-nak, de igazi arca már nincsen), ha robotok (*social bots*) erősítik a befolyásolást, bekövetkezik, amit Wolfgang Ischinger az információ fegyverként való használatának (*weaponization of information*) nevez. Ha az információból fegyver lesz, az igazság és a bizalom

forog kockán, márpedig mindkettő alapvető feltétele a társadalmi kohézióknak.

Az oroszok „reflexívkontrollnak” nevezik a hibrid fenyegetésnek azt a technikáját, amikor az áldozat erkölcsi vagy pszichológiai reakcióit használják ki, és már negyven éve alkalmazzák. „A reflexívkontroll információs műveleteket használ fel arra, hogy egy embert valamely döntésre készítsen, és közben azt higgye, hogy a sajátja.”^[35] Ez messze túlmegy a valóságmenedzselésről, mint jobbfajta PR-ról alkotott amerikai elképzelésen.^[36] Itt ismét felvetődik a kérdés: vajon ok-okozati összefüggés volt-e az oroszok 2016-os amerikai elnökválasztásokba való beavatkozása és Donald Trump elnökké választása között? Vlagyimir Putyin mindenesetre már 2007-ben, a müncheni biztonsági konferencián elmondott beszédével a világ tudomására hozta, hogy Amerika rendszerét sebezhetőnek tartja, káoszt és zavart okozhatna benne. A reflexívkontroll ez esetben eszköz lenne az amerikai lakosság irányítására anélkül, hogy a Kremlnek katonai erőszakhoz kellene folyamodnia. Ha így lenne, az orosz katonai vezetés mindenesetre elég rossz véleménnyel volna egy demokratikus társadalom értelmi képességeiről. A társadalomnak képesnek kell lennie, hogy felismerje a tényeket – az igazságot, mint Wolfgang Ischinger hangsúlyozza –, ennél fogva pedig „ésszerű és viszonylag helytálló, tapasztalatokon alapuló ítéletek” meghozatalára.^[37] A reflexívkontroll azonban kifejezetten érzelmi megrázkódtatást és nyugtalanságot igyekszik kiváltani – a véleményformálás céljával. Tényekről itt nincs szó.

Ezen a ponton szögezzük le: a vélemény és az értelem két különböző dolog. Amikor az értelem működik, az ember képes a belátásra, felismeri az (ésszerű) igazságot, és aszerint cselekszik;^[38] véleményt viszont rábeszélés hatására alkot.^[39] Ezért van az – világosít fel bennünket a politikai teória –, hogy az értelmi igazság a vélemény ellentéte.^[40]

Az igazság marginalizálásával és a rábeszéléssel közeli rokonságban áll a hazugság. Ha az igazság érzelmileg már nem mozgat meg bennünket, a hazugság egészen bizonyosan megteszi. A reflexívkontroll központi magvát a hazugság alkotja. Ahhoz azonban, hogy teljes hatása kibontakozhasson, szüksége van egy alapvető feltétel teljesülésére: a társadalomnak kondicionálva kell lennie a tömegpszichológia hatására. Ma a kondicionálás naponta sok órán át folyik, amikor önszántunkból kitesszük magunkat a reklámnak, az online platformok központi üzleti modelljének.

Egyébként Sigmund Freud egyik unokaöccse, a New York-i Edward Bernays volt az, aki feltalálta az imidzstanácsadást, és felfedezte a tömeglélektani hatásokat: „Az üzenetek – így Bernays – legyenek tömörek, egyszerűk, megjegyezhetők. Ha szövegek, akkor rövidek, például röplapok. Minden formájukban fontosak a képek, a plakátoktól egészen a filmig.”^[41] Ezt olvasva ugyan ki nem gondol akaratlanul is a Twitterre, a YouTube-ra, az Instagramra vagy a Snapchatre?

Twitterharcosok

Államok, amelyek más államokban katonai műveleteket hajtottak végre, még a 2000-es években is az információk őreiként léphettek fel, és hatékonyan kontrollálhatták, hogyan tudósít a média államközi konfliktusaikról. Az amerikai csapatok a 2003-as iraki háború során először osztottak be alakulataikba újságírókat. Ezzel ellenőrizhették, mit látnak és hallanak egy-egy katonai akcióból a riporterek, következésképpen pedig odahaza a tévénézők, az újságolvasók, választók és törvényhozási képviselők.

A média különösen konfliktushelyzetben használható jól arra, hogy az embereket az adott oldal mellett elkötelezze. Az internet előretörésével azonban ez a szerep odalett; civil zurnalistiként, online platformokon egycsapásra ki-ki politikai aktivitást fejthetett ki, háborús területekről tudósíthatott, a körülötte zajló eseményekkel összefüggő saját képeit és gondolatait terjeszthette a Twitteren és a Facebookon, és Twitter-harcossá válhatott.

A *Protective Edge* (Erős Szikla) elnevezésű izraeli hadművelet során – ami Izrael válasza volt három izraeli tizenéves 2014-ben végrehajtott elrablására és meggyilkolására – az akkor 16 éves palesztin lány, Farah Baker váratlanul sikeres civil újságíróvá lépett elő. Angol nyelvű tweetjei, amelyeket az Izrael által nagy erővel bombázott Gázai-övezetből küldött, gyorsan politikummá lettek, nap mint nap folyamatosan foglalkoztatták a világot, és formálták a közvéleményt a gázai háborúval kapcsolatban.

Farah családjával a Gázai-övezetben, apjának munkahelyével, az Al-Shifa kórházzal szemközt rekedt, épp amikor az izraeli bombatámadások 2014. július 28-án elérték csúcspontjukat. Ő ennek ellenére tudta tartani a kapcsolatot a külvilággal – a Twitteren. Már az előtt a bombazáporban töltött éjszaka előtt számtalan tweetet elküldött, és hangot adott véleményének: „BOMBING CHILDREN IS NOT OK” (Gyerekeket bombázni nem okés), [42] amivel 200 ezer követőre tett szert. Azon a júliusi éjszakán azonban egyedül félelmet fejeztek ki a tweetjei. Online sikolyát („I don’t want to die, I don’t want to die!” – Nem akarok meghalni! Nem akarok meghalni!) képek és audio-felvételek követték drónokról, mentőautókról, F-16-os harci gépekről, efféle jajkiáltások közé illesztve: „I AM CRYING AND I CAN’T STAND BOMBS SOUND!’ I might die tonight” – Sírok és nem bírom a bombák hangját! Lehet, hogy ma éjjel meghalok). [43]

Farah érzései, amelyek ezen az éjszakán a legnagyobb rettetté váltak, világszerte megindították az embereket, és mély rokonszenvet ébresztettek iránta. Megindító tweetjei még a hagyományos média lapjaiba is eljutottak, s Farah sokak számára azzá lett, aminek maga nevezte magát: „a gázai Anna Frankká” [44].

Az izraeliek számára Farah online aktivitása az első konfrontációt jelentette az ellenpropaganda digitális formájával, amire az izraeli hadsereg nagyon nem volt felkészülve. Farah civil újságíróskodása egészen új minőséget képviselt: narratívája nagy szimbolikus erővel rendelkezett, és sarkított történetet adott

elő, ami aligha lehetett volna ugyanilyen sikeres, ha egy negyvenéves palesztin férfi tweetelte volna a Gázai-övezetből.

Amikor a gázai háború 2014. augusztus 26-án egy egyiptomi közvetítéssel létrejött, határozatlan idejű fegyvernyugvással véget ért, katonai szempontból ugyan megnyerte Izrael a konfliktust, morális szempontból azonban az ország elveszítette a világ szemében.

A Farahéhoz hasonló civil újságírás nem minőségi zszurnalizmus. A civil újságírók tudósításai gyakran éppoly szuggesztívek, mint a katonai akciókról szóló propagandisztikus hírek; a civil újságírók ugyanis mindig csak a megélt eseményekkel kapcsolatos saját érzelmeiket és véleményüket adják vissza. Tudósításuk ritkán objektív, nem igen közvetít kendőzetlen tényeket.

„A vélemény szabad, de a hír szent”, írta Charles Prestwich Scott újságíró és szerkesztő már 1921-ben a *Guardian* száz éves fennállása alkalmából.^[45] Még a kilencvenes években is az ő szakmájabeliek gyakorolták a fő hatalmat a hírek felett: a hagyományos média többsége költségekokból ugyanazokat a híreket olyan ügynökségektől kapta, mint az AFP, a Thomson Reuters vagy a KNA, ennél fogva bizonyos mértékig szinkronizáltan működött; professzionális újságírók szelektálták, rövidítették, emelték ki a tartalmakat, vagy kérték ki róluk szakértők véleményét. Mivel pedig a hagyományos média mintegy a tudósítás oligopóliumával rendelkezett, törvényileg kötelezték arra, hogy demokratikus elvekhez igazodva és pluralisztikus módon tudósítsanak. Mielőtt a sajtó létrehozott volna valamit, ügyelt arra, hogy a kötelező gondossággal járjon el; sajtókódex követel-

te meg, hogy kötelezze magát a polgárok hiteles tájékoztatására. Még szigorúbban szabályozták a közszolgálati rádióadókat. Az állammal kötött rádiósz szerződés megkövetelte tőlük az objektivitást és a pártatlan, kiegyensúlyozott tájékoztatást. Még ha a magánadóknál nem alkalmazták is ugyanezt a szigorú mércét, azért egy alapszabály minden adó számára egyaránt érvényben volt: a politikai reklám tilalma. Választási hirdetéseket csak a választás előtt sugározhattak.

Ez a médiaetika egyáltalán nem vonatkozik a digitális információs térre, amely soha nem igényelte a tényeket: üzleti modellje ugyanis a reklám. A reklámban pedig szinte minden megengedett: a bagatellizálás, a túlzás, a kihagyás, az újradefiniálás, a hozzáköltés és a sima hazugság is.

A gumiszobában

A félprofesszionális civil újságírók, akiktől nem követelik ugyanazt a gondosságot, mint a hivatásosoktól, hivatkozhatnak a *laikusok kiváltságára*, vagyis támaszkodhatnak olyan sajtóközlésekre, amelyeket még senki nem cáfolt. Ez nem más, jelent, mint hogy ma bárki bármit sugározhat – kevés kivétellel, mert a politikai reklám tilalma a digitális információs térben is érvényes, amennyiben a hirdető ezért anyagi ellenszolgáltatást kap.

Amikor mindenki sugároz, hatalmas a zaj, *information overflow*, információ-túlcsordulás támad. A zaj megszűrése céljából az online platformok algoritmusokat alkalmaznak. A számítógé-

pes programok azonban a szerkesztőkkel ellentétben nem emberek, nem ismerik az információ kontextusát. Az emberek kontextusérzékenyek, a gépek (még) nem azok. Ez az egyik probléma. A másik, még nagyobb, hogy az algoritmusoknak, amelyekkel az online platformok rendelkeznek, a hagyományos média szerkesztőitől eltérően egyáltalán nem feladatuk, hogy demokratikus szempontok szerint és pluralisztikus módon szelektáljanak. Épp ellenkezőleg.

Csak azt szűrik és szelektálják, ami releváns, és nem csak az releváns, amire az online platformokon az információforrás igazságtartalmától és megbízhatóságától függetlenül jelentős igény mutatkozik – amit gyakran osztanak és lájkolnak –, hanem az is, ami saját magunkat a leginkább érdekel és saját véleményünknek megfelel. A 21. század tendenciózus véleménymédiáiként az online platformok pontosan ugyanolyanok, mint amik száz évvel ezelőtt a kommunista *Rote Fahne* vagy a náci *Völkischer Beobachter* volt. Egy online platform individualizált *newsfeed*-je (hírcsatornája) kizárólag azt jeleníti meg, ami az egyes emberek számára fontos. Így keletkeznek a gyakran emlegetett véleménybuborékok és visszhangkamrák; ezek életünk gumiszobái, amelyekből sem ajtó, sem ablakok nem nyílnak kifelé, a valóságra. A személyre szabott newsfeedek éppenséggel csak saját véleményünket és világképünket erősítik meg, nem mások, mint énünk tükrei. Az online platformokon keresztül barátaink sem érnek el bennünket már, ha mondanivalójuk a technológiával állig felfegyverzett automaták, az algoritmusok ítélete szerint kevésbé releváns.

A következmény: ma az egyes emberek ebben a töredezett digitális véleménytömegben a közös valóság megtapasztalása mellett a róla folytatott véleménycserét is nélkülözik. Kapcsolatainkat megzavarta az online platformok okozta atomizálódásunk.

„Vedd fel a Beats^x-fejhallgatódat, kapcsold be az Apple Music Streamedet, és tedd ezt a világot a saját világoddá”, fogalmazza meg az Apple cég egy 2017-es rádióreklámja. A te világod nem az én világom, még kevésbé az ő világa. Nincsen többé „mi”, s ugyanezért többé nem létezik a valóság közös érzékelése sem. Ehelyett a különböző világok áttekinthetetlen sokaságát és a vélemények tömegét rémes összevisszaságként érzékeljük, ha újra meg újra csak saját vélekedésünkben erősítettünk meg.

Nem tudjuk, hogy saját világunk mekkora távolságra van a valóságtól. Amit ugyanis a valóságról tudunk, a tömegmédiából, és gyakran az online platformokról tudjuk.

A tömeget számos digitális cég tette vállalkozói tevékenységének tárgyává. Crowdsourcing, crowdfunding vagy crowdwork az új, diszruptív üzleti modell, amelyek esetében egy szolgáltatást, amelyet korábban egyetlen vállalkozás végzett, szolgáltatók tömegéhez helyeznek ki.

Nem volt jó véleménnyel a tömegről sem a kommunikációs mágus Bernays, sem pedig propagandaelméletének 20. századi követői. Nem mintha a tömeg intellektuális képességeiben kételkedtek volna – Hannah Arendt ezzel kapcsolatban így ír:

„A tömegember legfőbb tulajdonsága nem a durvaság és az elmaradottság, hanem az elszigeteltség és a normális társadal-

mi kapcsolatok hiánya.”^[46] A szkepszis alapja jóval inkább az, hogy a tömegtársadalom – Arendt így folytatja – fragmentált, „atomizált” társadalom, amely „elszigetelt egyének”-ből áll.^[47]
^[48]

Az online reklámapar, amely minden egyes felhasználót egyénileg szólít meg, és a gazdaság, amely „1 darabos tételméretekkel” dolgozik, azaz törekszik a 4. ipari forradalom, az Ipar 4.0 digitalizált gyártási folyamatának lehető legnagyobb personalizációjára, nemcsak boldog fogyasztókat állít elő, hanem egy apró darabokra töredezett, kötődések nélküli társadalmat is, amiből hiányoznak a közös tapasztalatok, és az olyan valóság, amelyben minden polgára osztozik. A szociológusok „szingularitásnak” nevezik azt a különösséget és egyedülállóságot, amire napjainkban oly sokunk törekszik.^[49] A különös vonzó: az egészen különös nyaralás, az egészen különös pár cipő, a sajátos táplálkozásmód. Szingulárisnak lenni azonban ezt is jelenti: egyedülállósággal meglehetősen egyedül és elveszett vagyok. Kaphatok ugyan visszajelzést róla, de egyedi voltomat nem értelmezik helyesen, mert senki sem ugyanazt a tapasztalatot osztja meg velem.

A digitális társadalom fragmentált tömegrészekéből áll, sokmillió individuális, egyes véleményből, „amelyek közt egy közös világ hullott darabokra”^[50], és a szubjektív életvalóságok, amelyeknek többé nincsen közük a körülöttünk ténylegesen végbemenő valósághoz. Szingularitásokként többé nem találunk egymásra. Az információs tér adatainak, tényeinek, alternatív tényeinek és véleményeinek kakofóniája összezavar ben-

nünket, mi pedig dezorientáltak leszünk – el lehet képzelni, hogy milyen rossz előfeltétele a körülöttünk zajló történésekről szóló vitának és róla való politikai véleményalkotásnak.

A digitális platformok véleménybuborékai és visszhangkamrái felerősítik ezt az effektust.^[51] „Az énközpontú elkeseredettség [...] nem teremtett összetartozást”, ismétli meg újra és újra aktívan cselekvő demokratikus társadalommal kapcsolatos igényét Hannah Arendt.^[52] Kedvenc platformjain azonban tervszerűen vágyaink tartalmaival operálnak, hogy sok hosszú órán át csakis ezekbe mélyedjünk bele. Az internetipar vállalkozásai a – lehetőség szerint csakis saját – világunk erősen szelektív észlelését erősítik fel, egyszersmind pedig meg is erősítenek bennünket egyéni világlátásunkban. Ez hihetetlenül jó érzés. Minden, ami körülvesz, olyan, amilyennek akarom, és amilyennek elképzelem. Világomból kirekesztődnek a kisebbségi vélemények, a valóság képei és az ellentmondás, ezért nem zavarják a közérzetemet sem.

A tömegmédiák véleménymegerősítő hatása egyébként nem újdonság: Paul Felix Lazarsfeld médiakutató már 1944-ben leírta. A tömegmédia-tartalmak és az amerikai választói magatartás közti összefüggést kutatta, és meglepetésére azt volt kénytelen megállapítani, hogy a propagandának nem alkotóeleme a meggyőzés művészete, és az emberek nem propagandisztikus sugalmazás nyomán változtatják meg véleményüket – épp ellenkezőleg: a propaganda meglévő véleményünkben erősít meg bennünket. Ma az online platformok leginkább az egészen kicsiny „önreferenciális köröket”^[53] favorizálják, és egy olyan tár-

sadalom feltételeit teremtték meg, amely „saját korlátoltságának megszállottja”^[54], amely „Google-meghajtású”, „Wikipédia-függő” és „blogokkal van impregnálva”^[55], s amely szilárdan kitart amellett, hogy „az erős vélemények többé nem különböztethetők meg a tényektől”^[56].

A véleménytömeg megszervezése

A II. világháború után a tömegelmélet békülékenyebbnek mutatkozott, mint Edward Bernays idejében, és a sokaság kevésbé lenéző fogalmát részesítette előnyben. A sokaság a maga heterogén sokrétűségében sok individuumot és szingularitást fog össze.

Ha a sokaság szingularitásai között erős vagy gyenge kötődések alakulnak ki, hálózat jön létre. Hasonló típusú érdekek erős hálózata létrehozza a sokat emlegetett visszhangkamrát, sok érdekcsoport közötti gyenge hálózatok hidat verhetnek a sokféleség irányába, feltéve, hogy a résztvevők új nézőpontokra akarnak szert tenni.^[57]

„Hálózatok, mindenütt hálózatok”,^[58] mondogatják ezért manapság – helyesen. A hálózatiság a digitalizáció technológiai hajtóereje, amely embereket más emberekkel és dolgokkal – illetve dolgokat más dolgokkal – egyetlen megakomputerré, a „tömegkooperáció hálózataivá” köt össze.^[59] Olyan hálózatokká, amelyek az egyetlen szerveződési struktúrát jelentik a szingularitások számára; az összes individuum részt vehet bennük, mű-

vészek, munkások vagy menedzserek egyaránt, mindenki a maga különbözősége és egyenlőtlensége dacára. A hálózatok már csak ezért is mélységesen inegalitáriusak.

A hálózatoktól eltérően a digitális társadalom és ezzel a különálló, egyéni vélemények káoszként érzékelt tömege politikailag már nem strukturálható. Szerveződési struktúrákként első sorban a politikai pártok esnek ki.^{[60], [61]} Az „1 darabos tételmélet” korában mind nagyobb nehézséget jelent számukra, hogy ugyanazokat a magas támogatottsági adatokat ériék el, mint korábban. Már alig van ugyanis valaki, aki azonosulni tudna a pártokkal mint közösséggel. A véleménybuborékokban és visszhangkamrákban élt atomizált élet ugyanis túlságosan nagy elletmondásban áll ezzel. A pártok taglétszámának csökkenése tehát nem csak a demográfiai változás következménye: a digitális társadalom organizatorikus átalakulása is tehet róla. Mert hát egy szinguláris ember nem nagyon tud azonosulni olyan pártprogrammal, amelyet sokaknak kell támogatniuk. Érdekeink egyszerűen túlságosan egyénivé váltak, semhogy megférjenek egyetlen párt vagy szervezet fedele alatt – legyen az bármelyik.

Időközben a pártok is érzékelték, hogy habár az atomizált tömegtársadalom^[62] választása nem esik rájuk, a tömeg korántsem apatikus, mert szemlátomást aktivizálható – mozgalomként: „Mi vagyunk a nép!”, ahogyan a tüntetők skandálták az NDK végóráiban. Rögtön eszünkbe jut erről az olasz Öt Csillag Mozgalom, a Pegida, Sahra Wagenknecht baloldali német gyűjtőmozgalma, az *Aufstehen*, Marine Le Pen nemzeti gyűjtő-

mozgalma, a *Rassemblement National*, vagy Emmanuel Macroné, a *La République en Marche*. Mozgalmak azért jönnek létre, hogy elfoglalják a politikai terepet, és versenybe szálljanak a pártokkal. A mozgalmak akkor sikeresek, ha parlamenti helyeket szereznek, vagy saját körükből hoznak létre kormányt, ahogyan Franciaországban vagy Olaszországban történt.

Már a 20. század totalitárius vezetői is megértették, hogy a társadalmi tömeg nem juttatható hatalomra sem érdekképviselő, sem pártprogram révén – csakis mozgalomként. Valamely minimálkonszenzus, mint a világnézet vagy az ideológia lép a helyébe a sokféleség összefogására. A pártprogramokat aztán úgy dolgozzák ki,^[63] hogy a sokféleséget vagy figyelmen kívül hagyják, vagy „cikkakkos manőverezéssel [aláássák]”^[64]. Ilyenképpen még Donald Trump viselkedése is megmagyarázhatóvá válik – még ha kívülállók számára így sem lesz sokkal érthetőbb. Lehet, hogy a Fehér Házban, mint erről Michael Hayden, a CIA volt igazgatója beszámol,^[65] hiperkaotikus az ügymenet, ám ami a külső megfigyelő számára véletlenszerűségnek tűnik, talán nem más, mint egy olyan heterogén követői tábor igényeinek célirányos kielégítése, amely azt várja el, hogy ugyanazokkal a világnézeti jelszavakkal újra és újra stimulálják és mozgásban tartsák. Így az is beleillik a képbe, hogy Donald Trump a 2018-as időközi választások előtt félretette a kormányzati ügyeket, hogy „heti hat vagy hét napon át” választási kampányt folytasson azoknak a republikánusoknak az érdekében, akik rossz, vagy szoros választási eredménnyel voltak kénytelenek számolni.^[66]

Ami a világnézeti oldalt illeti, három közös nevező létezik, aminek révén egyesíteni lehet a nemcsak izolált, hanem önmagukra is hagyott egyénekből álló heterogén egyformaságot.^[67] Az első minimálkonszenzust a nacionalizmus hozza létre: „America first!” vagy „Italy first!”; az embereket minden különbségük ellenére együtt lehet tartani nemzeti hovatartozásuk és potenciális idegenellenességük révén.

Másodszor, egyetértés jellemzi a véleményalkotó tömeget az egész rendszerrel szembeni ellenséges hozzáállásában.^[68]

„Crooked Hillary Clinton! Csaló Hillary” – Donald Trump ezt a vádat csaknem kétezerszer, minden kínálkozó alkalommal hangoztatta. Mindnyáján ismerjük a „Merkelnek mennie kell!” jelszót is, amiben a kancellárasszony kormányzati teljesítménye fölötti utálkozás kapott hangot.

A véleménytömeg azzal, hogy elutasítja az establishmentet, azt az álláspontot képviseli, hogy azok, akik a társadalmat eddig reprezentálták, „valójában bolondok voltak, hogy a többit a szakadékba vezették”^[69]. Donald Trump ezt az üzenetet is szakadatlanul, imamalom-szerűen ismételteti a múlt század nyolcvanas éveitől: „A világ nevet Amerika politikusain. (...) Nevetnek rajtunk a butaságunk, és vezetőink [butasága] miatt”^[70], „[S]tupid how stupid are our leaders”^[71], és: „Vezetőink olyan hülyék.”^[72]

A harmadik minimálkonszenzussal, hogy a saját nemzet az áldozat, és a világ többi része a veszére tör, az újfasizmus ideológiájához kerülünk közel. Ellentétben egyik legnagyobb kritikusával, a 2018-ban elhunyt republikánus John McCainnel, Do-

nald Trump nem abból indul ki, hogy Amerika az erkölcsi vezető szerepét tölti be a világban, hanem immár évtizedek óta ismételteti: „Az Egyesült Államok volt évtizedeken át a persely, amit mindenki kifosztott. Az a sok más ország, a barátaink, az ellenségeink, a szövetségeseink ... Az ellenség, az ellenség.”^[73] Avagy: „úgy gondolom, sok az ellenségünk. Úgy gondolom, az Európai Unió ellenség [annak alapján,] ami kárt a kereskedelemben okoznak nekünk. Önök most nem [is] gondolnának az Európai Unióra, de az az ellenség.”^[74]

A leglelkesebbek sem hunyhatnak többé szemet afelett, hogy az olyan innovációk, mint a Facebook, a Twitter és társaik: nem semlegesek. Akkor támadják a liberális demokráciát, amikor már csak egyvalaki takarítja el a romjait, egyvalaki, aki nem pártprogramot, hanem világnézetet és ideológiát képvisel, aki a tömegeket állandó mozgásban és – a népvezérek jó érzékével – állandó izgalomban tartja, egyvalaki, akivel kapcsolatban 1787-es esszéjében már Alexander Hamilton, az Egyesült Államok alapító atyáinak egyike is óvatosságra intette kortársait, mondván: az ilyenek „demagógokként kezdik és zsarnokként végzik.”^[75] Az egyvalakiból már rég sok lett.

A félelem hulláma

- Félhetünk!!!
- Emberek, a Stachuson lőttek! Csak kettőt-hármat, de lőttek!

– Lőttek, nekem meg ott van a munkahelyem! Az eszem megáll!

– Nem nekem való már ez a világ. Az ember egyfolytában csak félhet...

Ez a péntek este nem olyan, mint a többi.^[76] Semmi nem olyan ezen a langymeleg nyári estén, 2016. július 16-án, mint szokott, azóta, hogy a müncheni rendőrséget 17 óra 52 perckor riasztották: az Olympia bevásárlóközpontnál lövések dördültek.

Münchent rövid időn belül lezárják. Aki már eseménytelen napokon is szenved a hihetetlenül túlszűfolt város gyötrelmes közlekedési káosza miatt, most még kevésbé jut előre – már U-Bahnnal sem. A város Marienplatz alatti katakombáiban a müncheni közlekedési vállalat a peronok melletti hangszórókon keresztül tudatja: „Rendőrségi közlemény: az U-Bahn-forgalom mind a hat vonalon leállt.”

Az állomások, amelyeken egyébkor a sínhálózat maximális terhelhetőségét megközelítő csúcsforgalom zajlik, most kísértetiesen üresek. Az utcákon viszont villogó kék lámpákkal mentő- és rendőrautók száguldoznak, a város felett helikopterek körözködnek. München még sosem élt át hasonló eseményt. Pedig még csak alig egy hete, hogy Nizzában egy merénylő teherautóval iszonyatos módon véget vetett az ünnepnapra nyüzsgésnek: nyolcvanhat embert ölt meg. A terrortámadás miatti rémület még súlyosan megüli a lelket: bárkivel megtörténhet.

18 óra 30-tól a müncheni rendőrségen már teljes ariadókészlet, erősítést kértek Hessenből, Thüringiából és Baden-Württembergből, valamint a terrorelhárítóktól: a német GSG9-

től és az osztrák Cobrától. Ekkor még csak annyi bizonyos, hogy az Olympia bevásárlóközpontnál valaki tüzet nyitott, és fiatalok haltak bele lőtt sérüléseikbe.

A fiataikorú tettes a müncheni rendőrséggel való első találkozás után gyalog, a bevásárlóközpontot körülvéő területen át eljut egy garázs tetejére, ahonnan egy közeli lakossal – Thomas Salbey kotrógéppkezelővel, aki erkélyéről úgy hallotta, mintha némi távolságból riasztópisztoly-lövéseket adtak volna le – trágár szóváltásba keveredik, aztán egy szomszédos erkélyre lő, ahonnan valaki filmezi a jelenetet. (Utóbb fel is tette a netre.) Amikor a fiatalember elhagyja a parkolótetőt, s közben elveszíti a mobilját, sikerül eltűnnie a házsorok közt, és bejutnia egy lakóparkba. A következő két és fél órára nyoma vész, mintha a föld nyelte volna el.

Közben 18 óra 49 perckor a müncheni rendőrségre befut a következő riasztás: a város közepén, a közbeszédben Stachusnak nevezett Karlsplatzon, az üzleti élet forgalmas helyszínén lövések estek. Az eseményről az első beszámoló 19 óra 02 perckor jelenik meg a Twitteren: „Épp a Stachuson vagyok, most itt is lőnek.”

További jelentések következtek.

„Worst case: 3 tettes sorozatlövő fegyverekkel, mindegyik menekül. Hogy lesz itt megint normális élet?”

„A központban valszeg több halott.”

Eddig csak egy tetthely volt ismert, mostanra azonban a rendőrségi helyzet is áttekinthetetlenné válik. Vajon a tettes tényleg elhagyta a bevásárlóközpontot a belváros és a főpálya-

udvar irányába, mint azt egyes médiák „meg nem erősítetten” terjesztették? Eszerint jó hat kilométert tett meg, és szabadon mozgott. Vagy talán több tettesről van szó, akik – hasonlóképpen, mint a 2015. november 13-i párizsi, a Stade de France, a Bataclan és több étterem elleni támadás esetében – a városban haladva válogatás nélkül lőnek az emberekre? Ámokfutóval vagy terrortámadással van dolga a rendőrségnek?

„Most meg már állítólag a sétálóutcában is történik valami!”

A Hofbräuhaus söröző előtti téren, a szabadtéri kávézó területén vendégek ülnek – köztük számos külföldi turista – és söröznek. A WhatsAppon és a Twitteren érkeznek a legújabb „hírek” az Olympia bevásárlóközpontnál történt lövöldözéssel kapcsolatban, és a hagyományos médiák szünet nélkül tudósítanak Bajorországból (még külföldön is), és „müncheni mészárlást” emlegetnek. A vendégeket azonban ez egyelőre még nem izgatja. A tetthely és a Hofbräuhaus közti távolság hét kilométer, annyi, amennyi a frankfurti állatkert és Offenbach közt.

Egyszer csak három meglett férfi ront be a térre félelmében ordítva. Rohannak, segítségért kiáltanak, majd hirtelen csattanások hallatszanak. *Shooting, shooting!*

Ami most következik, az ragadós pánik, az érzelmek felülírják az értelmet. Rémületükben felpattannak vendégek, és életüket féltve futásnak erednek. Padok és székek borulnak egymásra, poharak és korsók csattannak szét a kövezeten. Most már minden zaj lövésnek hallatszik. A sokaság tolongva igyekszik bejutni a vendéglőkbe, bukdácsolnak, elesnek, egymást tapossák, kiabálnak, az asztalok alá bújnak és ablakokat vernek be,

hogy a hátsó udvarokba és a szemközti utcákba jussanak. Magukkal rántják a külföldi vendégeket is, akik nem értik, mi történik.

„Lövések az Isar-Tornál és a Hofbräuhausnál.”

A Twitteren, Facebookon és WhatsAppon megjelenő kurta beszámolók közt újra és újra képek, videók tűnnek fel a városról, kevés szó kíséretében, kontextus nélkül, de mélységesen zavarba ejtőn – a közösségi hálózatok a legkitűnőbb nonverbális keveréket kotyvasztják össze ahhoz, hogy tömegpánikot váltsanak ki. Az érzelmek válnak a legfontosabbá, az értelem teljesen jelentőségét veszti.^[77]

Hogy a félelem megbénítja az agyat, az mélyen az emberi természetben gyökeredzik. Veszélyre azonnal, habozás nélkül reagálni kell. Menekülésre, megdermedésre vagy támadásra vagyunk programozva, de ha nem áll fenn veszélyhelyzet, minden ilyen reakciónk túllő a célon. Csakhogy ebben a pánikban Münchenben minden összejön: egyre több online jelentés, viszont csak kevés információ a tényleges helyzetről, ehelyett megrázó mobilfelvételek az okostelefonokról; másodpercenként felüvöltő szirénák; bevetett rendőrök, akik ekkor már harcászati alakzatban fésülik át a gyalogos övezetet, dörrenések és durranások hol innen, hol onnan, és mindezen felül a helikopterek lármája. Néhányak félelme magával ragadja a többieket, „miközben a manapság mindent lefedő közösségi hálózatok felerősítik és kiterjesztik a közösségi járványt”^[78]. A közösségi médiával folytatott interakció az, aminek következtében pánikba esnek az emberek ezen az éjszakán.

A félelem a müncheniek körében már csak azért is olyan dinamikusan terjed, mert az okostelefon a gondolatokat és híreket gátló tényezők és kontroll nélkül, valós időben, késlekedés nélkül jelzi ki, a hatást nem tompítja az időeltolódás. Hogy mennyire szoros a kapcsolat az okostelefon és a pánik között, az események egy női szemtanúja is tanúsítja: most pedig, hogy működik a mobilom, (...) most információkat akarok. (...) Az információszerzést az ember megváltásnak érzi, véget vet a bizonytalanságnak, ami annyira kikészítette.”^[79]

Nem sokkal este fél kilenc előtt, amikor a fegyveres ámokfutó, David S. elhagyja az Olympia bevásárlóközpont melletti lakópark mélygarázsának kerékpártárolóját, a rendőrség feltartóztatja. Ott fejezi be ámokfutását: maga ellen fordítja fegyverét. Mindössze néhány percre tombolt, de ez kilenc ember életébe került. A tizedik halott ő maga volt.^[80]

A drámai éjszaka azonban a müncheni rendőrség számára még nem ér véget. Ugyanabban a percben, amikor a tettes a rendőrök szeme láttára végez magával, egy rendőrségi sajtóközleményben először bukkan fel a „terrorgyanú Münchenben” mondat.^[81] A nyelv óriási hatással van az emberre. Egy fogalom bekerülését a digitális információs térbe többé már nem lehet meg nem történtté tenni. Az emberek szituációkat képzelnek el, az érzelmek az ellenkezőjükbe fordulnak, és nincs, ami ugyanilyen gyorsan megnyugtathatná a münchenieket.

A müncheni rendőrség csak másnap kora hajnalban szünteti meg a riadókészültséget. Az egyedülálló esemény feldolgozása még hónapokba telik. 17 óra 51 perc és éjfél között, amint a

rendőrség később utána számol, „4310 telefonos riasztás futott be, ebből 310 hívó jelentette, hogy 71 különböző tetthelyen terrorcselekmény történt”^[82]. „Fantomtetthelyen”, ahogyan ezeket a rendőrség szóvivője, Marcus da Gloria Martins nevezte. Azon az estén ugyanis halálos kimenetelű esetek mindössze egyetlen helyszínen voltak – a városban kitört lövöldözésekkel kapcsolatos minden más riasztás vaklárma volt.

„A fantomtetthely a mi szószüleményünk (...) – mondja a sajtószóvivő, aki azon az emlékezetes estén oly megnyugtatóan józanul viselkedett, mint senki más –, ugyanis ez a jelenség ilyen intenzitással és mennyiségben még soha nem fordult elő, és mert ezek közt az eseményhelyszínek közt egy sem akadt, ahol bármi is történt volna.”^[83]

Csak a magamfajtákban bízom

Első ránézésre a müncheni ámokfutás felelevenítése nem illik egy olyan könyvbe, amely államközi konfliktusokkal és az államok külső kapcsolatával foglalkozik. Egy fiatalember bűncselekményt követett el, ami a rendőrség, mint belbiztonsági hatóság illetékességi körébe tartozik. Az ámokfutással összefüggő események azonban megérdemlik a figyelmünket. Ugyanis azt szemléltetik, hogy miképpen válthat ki az online interakció dinamikus, előre nem megjósolható viselkedést a lakosságból.

Megállapítottuk: az online platformokon mindenki mindent továbbít, mindenki verseng a lájkokért. Ennek során egy-egy je-

lentés igazságtartalma semmiféle szerepet nem játszik. Amikor a *Süddeutsche Zeitung* egy kutatóteamje két hónappal a müncheni ámokfutás után felkutatta és kérdőre vonta a Stachuson eldőrdült lövésekről szóló első tweet küldőjét, az illető lakonikusan csak ennyit mondott: „A dolog neve közösségi média, és az igazság ott nem feltétlen téma.” És: „Az igazságot amúgy se fogjuk megtudni.”^[84]

A civil tudósítók egyvalamiben bizonyosak: a legtöbb pontot az gyűjtheti, aki a lehető leggyorsabban számol be válságokról vagy merényletekről, függetlenül attól, hogy hitelesen teszi, vagy sem. A veszélyekről és katasztrófákról szóló különleges jelentések azok, amik szalagcímmé válnak és gyorsan elterjednek.

Terjedésüket az ember egyik legerősebb elemi érzelme ösztönzi: a félelem. Hogy milyen erős érzelem az ember félelme, Heinz Bude szociológus egyetlen rövid mondattal fejezi ki: „A félelem az az elv, amely abszolút módon uralkodik, amikor minden más elv viszonylagossá vált.”^[85] Ilyenkor úgy érezzük magunkat, mintha sötét erők vették volna át felettünk a hatalmat, és mintha tehetetlenül ki volnánk szolgáltatva alig felfogható – a terrorizmustól a mesterséges intelligenciáig terjedő – erőknek. Elkerülhetetlen, ami erre következik: a dolgok túlreagálása, ahogyan az a müncheni lakosság esetében is megfigyelhető volt.

Mivel a félelem és elbizonytalanodás politikai szempontból hasznos állapot, ennek a fiatal évszázadnak egyre több politikus állt át arra, hogy tudatosan félelmeket gerjesszen. A félelem és létünk fenyegetettségének korszakában élünk, jóllehet

hosszú évek óta tartó gazdasági fellendülés és alacsony munkanélküliség biztosítja jólétünket, a bűnügyi statisztikák azt jelzik, hogy a bűncselekmények száma csökken, és élettartam-kilátásaink évről évre több héttel javulnak – azaz minden jel arra mutat, hogy nagyon biztonságos időkben és térségekben élünk, ahol éppen hogy nem kell félelemnek uralkodnia. Ha a félelem és bizonytalanság érzése ennek ellenére patológikussá válik – hiszen tényleges indoka nincsen –, akkor az az ellenkező előjelű érzelem, a bizalom hiányára utal.

A bizalom az a kötőanyag, ami egy társadalmat összetart, s egyúttal a demokrácia létfontosságú alapja. Az Edelman Trust Barometer világszerte évek óta regisztrálja, mennyire bíznak az egyes országokban élők különböző intézményekben.^[86] Ha a gazdaságba vetett bizalmat nézzük, ebből a legtöbbet a technológiai vállalkozások, a legkevesebbet a bankok élvezik.

Államról államra jelentősen ingadozás tapasztalható a tekintetben, hogy mennyire bíznak a polgárok az állami intézményekben. Az Egyesült Államokban 2018 folyamán a polgárok bizalma soha nem látott mértékben csökkent. Az amerikaiak 59 százaléka nyilatkozik úgy, hogy saját kormányát az egész ország messze legrosszabbul működő szervezetének tartja. Érdekesek a nagy ellenlábás, Kína adatai: ugyanezt a kínaiaknak csak 10 százaléka gondolja a kínai vezetésről. Azt, hogy a kormányzat az államot egy jobb jövőbe vezeti, Kínában a lakosság 68 százaléka hiszi, ezzel szemben az Egyesült Államok polgárainak csak 15 százaléka.

Elgondolkodtató, hogy a számok látszólag a demokrácia ellen és a diktatúra mellett szólnak. De vigyázat: ez esetben az empirizmus csapdája fenyeget. Amit a pusztá közvéleménykutatási eredmények valószínűsítenek, az a diktatórikus rezsimek fölénye a liberális-demokratikus berendezkedésekkel szemben. Az autokráciák stabilabbaknak tűnnek, mint a demokráciák, azonban arról, hogy stabilitásuk elnyomó intézkedéseken, folyamatos ellenőrzésen és elnyomáson nyugszik, az adatok mit sem mondanak. Különösen a nyugati gazdaság és ipar szereti ezt figyelmen kívül hagyni. A kínai gazdasági csoda már évekkel korábban lelkesedéssel töltötte el a Nyugatot, most pedig mindenki ámul, hogy Kína, immáron a digitális fejlődés következő szakaszának éllovasa, négyszer gyorsabban hoz létre termékeket és gazdasági modelleket, mint a Szilícium-völgy. Noha egyre több aggály vetődik fel Peking politikai gyakorlatát illetően, mifelénk még mindig szeretnének hasonlóan jelentős gazdasági sikereket felmutatni.

Az Egyesült Államok 2018-ban a politikai intézményei iránti bizalom mindmáig példátlan fogyatkozását volt kénytelen elkönyvelni; a bizalom eltolódott az intézményektől a hasonló fel fogású emberek felé: „Ez olyan, mint én vagyok, ebben megbízhatom.”

Az utazási ajánlatok az Airbnb-n, a termékértékelések az Amazonon, az étteremtippek a Yelpen – mind-mind hitelt érdemlőbbnek tűnik, mint a hivatalos közlemények vagy a sajtó-beszámoló. „Olyan világban élünk, ahol fokról fokra jobban megbízunk Facebook-barátainkban és a twitteres tömegben,

mint a Nemzetközi Valutaalapban vagy a miniszterelnökben”, [87] és azok közé, akik ilyen bizalmat élveznek, éppúgy beletartoznak a müncheni ámokfutás civil tudósítói, mint a gázai Farah Baker. A felülről származó igazsággal szembekerül az alulról jövő.

De ez is hozzátartozik a populista filozófiához, amely a tömeg, a hallgatag többség bölcsességét fölébe helyezi a vélelmezetten korrupt establishment bölcsességének, és megvetően elutasítja a szakértőket, értelmiségieket, fennálló intézményeket és az eliteket. [88], [89]

Pedig amit számunkra ismeretlen személyek az információs térben posztolnak, csak ritkán tárgyyszerű hír. Amiről hitelesen tudósítanak, azok a saját érzelmeik. Ahol empatikus közönséget találnak, oda érzelmek újabb hullámát zúdítják. Érzelmileg érintenek meg másokat, így viszik át rájuk saját kedélyállapotukat, miközben olyan erővel képesek mozgósítani a befogadókat, hogy az adott érzés tömegekre terjed át – olyan folyamat ez, amelyet *viral*nek, „járványszerűnek” is neveznek.

Megérinteni és megérintetni: ami ösztönösen úgy hangzik, mint amit mindannyian szeretnénk, odavezetett, hogy egyre több ember vesz igénybe online platformokat hírigényeinek kielégítésére. Globálisan nézve csökkent ugyan kissé a hírek online hálózatokról való beszerzése, ez a csökkenés azonban nagyon egyenetlenül oszlik meg számos ország között, ugyanis a digitális információs tér felhasználóinak száma még mindig nő [90] – végül is könnyen hozzáférhető és ingyenes.

Ugyanakkor az online platformok azok, amikben csak elővigyázattal volna szabad megbíznunk. A digitális információs térben a messzemenő anonimitás alig teszi lehetővé a források ellenőrzését. Vajon csakugyan az-e valaki vagy valami, akinek vagy aminek kiadja magát? Vajon ember, vagy robot? Mindenesetre az online platformokon nem számíthatunk minőségi újságírássra, olyanra, amelyiknek alapja a források felülvizsgálata, a hitelességük ellenőrzése, olyanra, amelyik híreket gyűjt, és torzítatlanul ad tovább.

Valóság és mese határán

„Lemondani a tényekről annyi, mint lemondani a szabadságról. Ha semmi sem igaz, akkor senki sem bírálhatja a hatalmat, mert nincs, aminek alapján megtehetné. Ha semmi sem igaz, akkor minden csak látványosság.”^[91] Az amerikai Timothy Snydernek, a kelet-európai történelem professzorának ez a felfogása alighanem a digitális világba beleszületettek (*digital natives*) tetszését nyeri el legkevésbé. „Olyan szabadnak érezzük magunkat, mint korábban soha”, állítják ők. Aki a digitális korszakban nőtt fel, már nem tudja elképzelni életét online platformok nélkül. Illúzió híján a *native* unatkozik, miként az az ifjú író, aki a közösségi hálózatok, fikciók és a demokrácia közti összefüggést így foglalja össze: „Szeretjük a Facebookot. Akarjuk, hogy hazudjanak nekünk. Végre megint történik valami. Hisz ez a demokrácia olyan unalmas.”^[92] A közösségi hálózatok teli vannak

provokációval és fikcióval. Az élet, a politika, a társadalom – ezt próbálják elhitetni – lehetne sokkal, de sokkal tökéletesebb foltok, ráncok és repedések nélkül, vagy anélkül a sok délről jövő idegen nélkül.

A valóság és a mese közötti határ nem csak az információs térben tűnik el, hanem a környezeti intelligenciában is, ahol mesterséges intelligencia jelenik meg és cselekszik az ember helyett. Amikor a Google bemutatja Duplex nevű beszélő asszisztensét, amely helyet foglal telefonon éttermekbe és fodrászatokba, a felhívott számára azonban nem azonosítható az embernek csupán csak fikciójaként, akkor a valóság más, mint amit a beszélgetőpartnerrel elhitetnek. A Google Duplex ún. *deep fake*-rafináltan hazudó robot, hiszen elhallgatja, hogy gép. Fikciót él át az ember a virtuális valóságban is, amikor zárt térben tartózkodik, de VR szemüvegének és egy szenzoros kesztyűnek köszönhetően erdei- vagy űrsétára indul, élete párjával fiktív tengerparton vakációzik, ahol különösen kék a tenger, zöldek a pálmák, és az égen három Nap ragyog. Csakhogy a felhasználó szabadsága – vagyis hogy a digitális transzformáció valamennyi fikciójába és meséjébe beléphet, és fogyaszthatja őket – nem egyezik a civil emberével, annak előfeltétele ugyanis az igazság.

Az állampolgár része egy politikai közösségnek, ez pedig „az értelemmel megáldott emberek közösségeként”^[93] értendő, amely tartalmazza az ész politikai alapelvét.^[94] Ennek, mielőtt értelmes döntéseket hozhat, tényekre van szüksége, amelyek mindenki számára közösek, igényli „azt a közöset (...), amiben

mindnyájan egyek lehetnek, akik a szabadságot akarják, hogy azután politikai tevékenységben (...) fejthessenek ki hatást”.^[95]

A digitális információs térben fennáll a veszélye, hogy elsikkad az igazság és a politikai közösség. Aki voltaképp egy politikai közösségben kívánna részt venni, az egy hallatlanul izgalmas digitális cirkusszal hipnotizáltatja magát. Aki vitatkozna, hagyja, hogy botrányok és tabudöntögetések hatása alá kerüljön. Aki csak felizgatja magát, többé nem beszél, mert az érzelmi töltet nem készítet visszakérdezésre.^[96] Ez a fikció vagy az alternatív tények legfőbb hatalma: veszélyezteti a társadalmi békét. Tulajdonképpen pontosan ezt a leckét kaptuk már 2002-ben, az amerikaiak Irakba való bevonulásával.

Ha sikerül eltorzítani az igazságot, elködösíteni a valóságot, egy hibrid támadás az információs térben máris sikert könyvelhet el. Wolfgang Ischinger ezért beszél „háborús ködről” (*fog of warról*): „Mára oda jutottunk, hogy a háborús köd háborúmentes időkben is létezhet. A háborús köd a társadalmi élet normális részévé lesz. (...) Hogy zszurnalisztikusan fokozzuk: az igazság kiderítése terén folyamatosan háborút folytatunk. Az igazság elplezése, amire korábban csak háború idején, vagy kevéssel a háború fegyvereinek bevetése előtt került sor, ma mindennapos.”^[97]

A már említett Podesta-kiszivárogtatás annak is jelképes példája, hogy nemcsak a hazugság, hanem az igazság is okozhat károkat. Lehetetlenné válik ugyanis a jövő tervezése, ha nincs egy védett tér, amiben a diszkréció az úr. Ha a személyes tervek és stratégiák – üzleti titkoktól a kormányok terveitig – nyilvános-

ságra kerülnek, elvesztik az erejüket, és tárgytalanná válnak, érvényüket veszítik. „Akkor a tervek mehetnek a szemétkébe”, állapítja meg helyesen Wolfgang Ischinger.^[98] És ez az a tulajdonképpeni kár, ami Hillary Clintont 2016-ban az orosz hekkertámadás következtében érte: az elnöki poszt felé vezető úton egy választási stratégia abban a pillanatban értékét veszti, hogy nyilvánosságra kerül, és az ellenfél alkalmazkodhat hozzá.

Hogy a lakosságnak politikai érdeke fűződik a titkok kiderüléséhez, az azért van, mert a titoktartást a hatalommal kapcsolja össze. „A hatalom ott kezdődik, ahol a nyilvánosság véget ér”, állapítja meg már Hannah Arendt is.^[99] Ezért az, ami titkos, gyorsan az összeesküvés hírébe hozható, összeesküvés-elméletekkel pedig jól magyarázhatók a történelem és a jelenkor megmagyarázhatatlan eseményei.

Hogyan sikerült hát Hillary Clinton ellenfeleinek, hogy megfosszák a hatalmától? Az orosz ügynökök, akiket vádiratában Bob Mueller amerikai különleges ügyész név szerint felsorolt, nem sajnálták az időt, hogy alaposan megtervezzenek egy hatásos kampányt az olyan demokraták, mint John Podesta vagy az elnökjelölt eredményes diszkreditálása céljából, azaz hogy megdolgozzák a nyilvánosságot. Ehhez a támadók létrehoztak egy új hamis identitást is: a DCLeaks-et. A DCLeaks.com internetes debütálását, amelyet lejárató kampányukkal összefüggésben készítettek elő, bitcoinban fizették. Az oldal végül 2016 júliusában kezdte meg működését azzal, hogy nyilvánosságra hozta a demokrata tábortól ellopott e-maileket, és 2017 márciusáig – ekkor zárták be – több mint egymillió letöltést könyvelhetett el. Nép-

szerűségét az ideiglenes jelleggel létrehozott DCLeaks-Facebook-profilnak és a @dcleaks_. Twitter-fióknak is köszönhette. A két közösségi hálózaton való jelenlét a DCLeaksen publikált dokumentumok láthatóságát volt hivatva fokozni. Az egykor kommunista Oroszország szemlátomást nagyon jól megértette, hogyan működik a reklám a 21. században.

A dolog azonban nem állt meg a passzív kommunikációnál, aminek során a vádlottak egyszerűen csak közzétették, ami a kezükbe került. A hamis identitású Guccifer 2.0 órája akkor jött el, amikor a lopott információkat proaktív módon elküldték lobbistáknak és a médiának. A 2016-os kongresszusi választások egyik jelöltje kifejezetten érdeklődött Guccifer 2.0-nál, vajon kaphatna-e információkat demokrata versenytársairól. Guccifer 2.0 rögtön megosztotta az illetővel a kért dokumentumokat. A Trump-kampány egyik közreműködőjével még egyfajta dialógus is kialakult, és Guccifer felajánlotta segítségét: „Please tell me if i can help u anyhow ... it would be a great pleasure to me” (Kérem, közölje, ha bármiben a segítségére lehetek ... nagy örömmre szolgálna).

E tevékenységek során Guccifer 2.0 a lopott anyagot az „Organisation 1” felületére töltötte fel – amelynek neve a vádirat szerint a WikiLeaks helyett állt –, és azzal kezdte, hogy eszmecserét folytatott a szolgáltatóval, mikor lenne a legmegfelelőbb a megjelentetés a nyilvánosságra tett hatás szempontjából. Leleplező platformnak az „Organisation 1” volna a legmegfelelőbb, javasolta, hogy a közzététel minél nagyobb hatótávolságú és hatású legyen.

Milyen szerepet játszott Donald Trump junior a lopott anyag WikiLeaksen való nyilvánosságra hozatalában? A Trump fiú közösségi hálózatokon keresztül szórványos kapcsolatokat tartott a WikiLeakszel, és „úgy tűnik, szinkronizálta a választási kampány akcióit [ti. az apjáét] a WikiLeaksével”^[100]. Egy 2016. július 27-i sajtótájékoztatón még buzdította Oroszországot: „Oroszország, ha halljátok, amit mondok: remélem, képesek vagytok rá, hogy megtaláljátok a 30 ezer hiányzó e-mailt. Szerintem a sajtónk gazdagon megjutalmaz majd érte benneteket”,^[101] s ezt a Hillary Clinton külügyminiszteri időszakából való e-mailekre értette, amelyeket az elnökjelölt-asszony letörölt magánszerveireiről.

Az oroszoknak nem kellett ezt kétszer mondani. Alig néhány óra múlva már megpróbáltak betörni Hillary Clinton privát számítógépeibe.^[102]

Mivel a hírszerző szolgálatok mindig is gyűjtöttek információkat ellenfeleikről, az az információ, amit az ellenfél számítógépeiről lopnak vagy más módon szereznek meg, majd nyilvánosságra hoznak, maga is fegyverré lehet.^[103] A voltaképpen titkos tények leleplezésének műveletét *doxing*nek nevezik. A kikémlelt fájlok nemcsak gazdaságilag releváns adatokat vagy szellemi tulajdont tartalmazhatnak – ezt illetően a gazdasági kémkedés területén mozgunk –, hanem igencsak személyes információkat is, amiket nem a nyilvánosságnak szántak. Rossz fényt vethetnek a feladóra vagy a címzettre, ha bosszúság, düh, csalódás fogalmazódik meg bennük, vagy ha betegségekkel kapcsolatos információk szivárognak ki, a levelezésben kompromittáló fo-

tók találhatók, netán a kommunikációból jogellenes magatartásra lehet következtetni.

Az európai parlamenti választási kampány utolsó napjaiban, a 2019. május 26-i, vasárnapi szavazás előtt egy héttel ilyen *doxing*-bomba robbant Európa közepén, Bécsben. Ezúttal éppen olyasféle feltörekvő politikusok lettek a támadás célpontjai, akik szívesen alkalmazzák az online platformokat politikai ellenfelek lejáratására.

2019. május 17-én ismeretlen személyek egy titokban forgatott leleplező videót juttattak el a *Süddeutsche Zeitung*hoz és a *Spiegel*hez, amely az FPÖ későbbi osztrák alelnökéről, Heinz-Christian Strachéről készült, miközben ibizai vakációján meghitt, privát közegben egyebek mellett a sajtószabadsággal kapcsolatban nyilatkozik meg, ekképpen: aki az osztrák *Kronen Zeitung*ot uralja, az képes irányítani a közvéleményt. Aki ráadásul egy tévéadót is kontrollál, „mindent” meghatároz. Ha például egy orosz oligarcha megvenné a *Kronen Zeitung*ot, mint valami futballklubot, szükségessé válna a lapnál a politikai barátok megerősítése és az ellenfelek onnan való elbocsátása.

Az osztrák alkancellár antidemokratikus kijelentéseire azért kerülhetett sor, mert ismeretlenek a felvételt megelőzően *social engineering*et folytattak, azaz felderítették a célszemély környezetét, majd pedig egy bizonyos fajta viselkedésre készítették. Erre is ugyanaz érvényes, mint a már említett reflexívkontrollra: az információ értékét az adja, hogy kihatással van a jövőre. Hogy tudhatók az ellenfél gyengéi, amelyeket egy bizonyos magatartás kiprovokálása érdekében aktivizálni lehet. Jelen eset-

ben a „gyengék” egy vonzó szőkeségből, egy teli pénztárcából, emellett nyilvánvalóan sok alkoholból álltak össze. Ezúttal is feltűnő a nyilvánosságra hozatal időpontja: pénteken este került rá sor. Tudható volt, hogy egy teljes hétvégén keresztül egész Ausztria, és talán egész Európa az *Ibizagate*-ről vitázik és spekulál majd, így aztán az ügy az európai választásokig egészen bizonyosan nem megy majd feledésbe.

A tanulság: a *social engineering*gel vagy a *doxing*gal szemben egyik politikai oldal sincsen biztonságban. Bárki ellen bevetethetik. Politikailag bárki elintézhető, mert időközben mindenki megtanulta, hogyan alkalmazzon hatékony hibrid eszközöket politikai ellenfeleivel szemben. Egyedül az az érdekes kérdés nyitott még, hogy ki volt az, aki a „rejtett kamerával” kapitális osztrák kormányválságot idézett elő. A rejtélyt mindmáig nem sikerült maradéktalanul megoldani.

A felvilágosodás vége

Az online platformoknak, azaz a 21. század tendenciózus véleménymédiáinak hatására egyre rosszabb állapotba kerülnek a demokratikus berendezkedésű államok egykoron tündöklő csilagai. Az amerikai alkotmányjogászok mindinkább egyetértenek abban, hogy az Egyesült Államok mára már működésképtelen demokráciának sem mondható, hanem legfeljebb egy hibrid rendszernek a működésképtelen demokrácia és diktatúra kö-

zött, ami már csak az uralmi formák legaljára, a despotizmusba csúszhat le.^[104]

A veszély igencsak valóságos, mert a digitális véleménytömeg könnyen felingerelhető, egyaránt hallgat a jobb- és baloldali szélsőségekre, hagyja, hogy a hálón kollektív szereplőként egy világnézet égisze alatt mozgalommá szervezzék, és a legerősebbhez igazodik, aki a véleménytömegből kiemelkedve úgy tesz, mintha e tömeghez tartozna. Az olyan jó szimatú tömegvezér, akinek egyszerű válaszai vannak bonyolult összefüggésekre, aki megváltást ígér az irányultság nélküliség alól a véleménytömegnek – miközben pedig saját nagyszerűségét és tévedhetetlenségé hangoztatja –, néhány éve is még elképzelhetetlen lett volna a nyugati demokráciákban.

A demokratikus hanyatlást nemcsak a 21. századi digitális tömegtársadalom gyorsítja, hanem a posztmodern kor ideológiája is, ahogyan az a tudományok területén mindenütt megnyilvánul.

„Haragszom tudós kollégáimra, mert egy posztmodern elmélet követői, és azt állítják, igazság nem létezik”, jegyzi meg a témával kapcsolatban Jean-Marc Rickli svájci védelmi szakértő.^[105] Az objektív valóság tagadását Rickli a tudományok teljes kudarcának tartja. A kutatás és a tudomány, valaha mindkettő az igazság garanciája volt, ma a valóság önmagától „elidegenedett konstrukcióját” kultiválva elméleti alapokkal szolgál annak megokolására, hogy a tények mellett miért létezhetnek alternatív tények. Valamennyi narratíva „egyenként érvényesen” áll egymás mellett, akkor is, ha igazság mellé vélemény társul. Még

rosszabb, hogy az igazságok véleményekké bomlanak fel, és az a körülmény, hogy az emberek rendelkeznek a hazugság képességével, teljesen eltűnik az emberek tudatából.^[106] Elveszítjük a különbségtételre való képességünket, nem értjük már az igazság és hazugság közti különbséget, és nem vesszük észre, hogy emberek nemcsak az igazat mondják nekünk, hanem hazudhatnak is.

Ezenközben egyre több amerikai gondolja úgy, hogy a Föld lapos. Pedig tudhatnák, hiszen az emberi értelem némi megfeszítése árán rá lehet jönni az értelmi igazságra: a Föld golyó, amely a Nap körül kering. Ám nem egy Homo digitalis inkább hajlik a tévedésre vagy a tudatlanságra, ami ellentéte az értelmi igazságnak,^[107] és észérvekkel sem megközelíthető. Még egyszerűbb azonban letagadni, elhallgatni vagy megváltoztatni a dologi igazságokat, például azt, hogy az orosz kormány befolyásolta a 2016-os amerikai elnökválasztásokat. A dologi valóság az informatikai befolyásoló műveletek első áldozata, és megeshet, hogy ismételt tagadások nyomán végül teljesen semmivé válik.

A sok valóság állítólagos egymás melletti létezésének indoklásával a modern agykutatás is szolgál. Mindennel, ami körülvesz bennünket, mondják a neurocentrizmus hívei, csak az agy ámit bennünket, pedig az testünk neurokémiai folyamatainak eredménye. Vajon egy erdő lombja akkor is susog, ha a susogást éppen nem hallhatom, mert a városban tartózkodom? A neurocentristák azt sugallják, hogy egy fa és lombjának susogása csak azért materializálódik valóságként, mert érzékszerveink megengedik. Minden, amit egy ember tud vagy átél, érzéki tapasztá-

láson nyugszik – hangzik a tételük. Amit az érzékek nem közvetítenek, nem létezik. Röviden, az embert, úgymond, agyának neurokémiai folyamatai determinálják. Valójában semmi nem létezik körülötte a valóságban, ha nem összpontosítja rá az érzékeit.^[108]

„Minden illúzió”, folytatja ezért a dohogást a katonai teoretikus Rickli.^[109] Szerinte különösen az európaiakat fertőzte meg ez az ideológia. „Ha minden csak szubjektív konstrukció, és nem létezik már objektív igazság, akkor alternatív igazságok jelennek meg. Akkor az emberek hozzászoknak az alternatív tényekhez. És a tudomány ezt még támogatja is.”^[110]

A felvilágosodás és az értelem korának végén vagyunk, írja Henry Kissinger is a mesterséges intelligenciáról szóló figyelemre méltó esszéjében.^[111] A felvilágosodás egykor az emberi megfigyelésnek rendelte alá az igazságokat, felszólította az embert, hogy maga gondolkodjék és elemezze a valóságot. De hogy milyen súlyos helyzetbe jutott a felvilágosodás, amelynek a szabad emberről alkotott képe mélyen beépült európai jogrendünkbe, kitűnik az értelem bukásáról kialakult széles egyetértésből.

Jean-Marc Rickli kitekintéssel szolgál arra nézve, mi következhet ezután. A valóság önmagától elidegenedett konstrukciójával az emberiség eljut „a felvilágosodás végéhez. Ez a korszak befejeződött. Az értelem helyébe az érzelmek léptek”^[112]. És hogy mit jelent még a sokféle különböző valóság létezése közös jövőnk szempontjából, amikor az ember nem kapaszkodhat többé az egyetlen igazság horgonyában, ami a felvilágosodás során

az értelmi igazság volt, a felvilágosodás előtti Európában pedig a hit? Jean-Marc Rickli mélyen vallja:

„A jövő az én szememben olyan, mint a mátrix.”^[113] Komputerszimulációs látszatvilág, ami valóság mindenki számára, aki benne él, ám megtévesztésként lepleződik le az előtt, akinek sikerül megszöknie belőle.

Vigyázat, nyelv! Provokáció és extrémizmus

„Folyik a politikai kommunikáció általános tálibosítása. Aki azt akarja, hogy észrevegyék, csak egyetlen eszközzel érheti el: provokációval. Ezért nem létezik többé konszenzusorientált politikus, hanem csak szélsőséges. Szélsőséges Vlagyimir Putyin, szélsőséges Hszi Csin-ping, Mohamed bin Szalman és Recep Tayyip Erdoğan is.”^[114]

Az, amit Heiko Borchert svájci védelmi miniszter a politikai kommunikáció tálibosításának nevez, a nyilvánosság digitális irányú struktúraváltásának tünete. A tálibosítás fogalma itt azt jelöli, hogy a politikai kommunikációból kiküszöbölődnek az értelmi és dologi igazságok, izgalom és túlingerlés lép a helyükbe. A 19. Bundestag ülései beszédesen tanúsítják ezt. „Érvek ütköztetése helyett viharos jelenetek” és „eltúlzott színpadiasság” határozza meg a „Tisztelt Ház” üléseit, ezek provokálását az AfD, amely csak 2017 óta képviselteti magát a Bundestagban, írásban lefektetett stratégiájának tette meg.^[115] Egyedül a ribillió számít.

A botránygerjesztéssel a józan tények csak ritkán képesek versenyre kelni. Alig keltenek izgalmat vagy érzelmi hatást, gyakran egyszerűen csak szárazak és avítottak. A valóságos dolgok ráadásul kényelmetlenek is, tehát nem nevezik nevükön, hanem inkább elbagatellizálják őket. Aki az elbocsátások szót a karcsúsítással helyettesíti, probléma helyett kihívásról beszél, a visszaesést negatív növekedésnek nevezi, vagy a hazugságokat alternatív tényeknek minősíti, megváltoztatja az emberek gondolkodását. A túldramatizált és agresszív megnyilatkozások – a sajtó a nép ellensége, a választásokat manipulálják, a kormány egy fertő, a jogrendszer: vicc – befolyásolják az emberi gondolkodásmódot. Ma, állapítják meg nyelvtudósok, a német nyelv ismét nagyon hasonlít „a weimari köztársaság végnapjainak” nyelvéhez. És ahogyan akkoriban, most is szembetűnő a nyelv és a fizikai erőszak összefüggése. „A nyelv az erőszak előtt jár.”^[116] Jobboldali csoportosulások tüntetései indulhatnak nyugodtan, de abban a pillanatban, amikor elkezdődik a jelszavak skandálása, a demonstrációk gyakran átcsapnak erőszakos rendzavarásba.^[117]

A tálibosításról azonban a beszédhelyzettől függően a terroristikus erőszakra is asszociálhatunk: ilyen értelemben a tálibosított kommunikáció nem más, mint terrorizmus az információs térben. Az ékesszóló meggyőzés helyébe a sértés lép – valamint a zsarolással, szexuális erőszakkal, sőt a halállal való fenyegetés. „Soha többé ne fenyegetse az Egyesült Államokat, vagy olyan következményekkel kell számolnia, amilyeneket a történelem során csak kevesen voltak kénytelenek elviselni.

Nem vagyunk többé az az ország, amelyik tudomásul veszi az ön erőszakot és halált idéző örült szavait. Legyen óvatos!!”^[118]
Vagy: „Senki, aki Iránnal üzletel, nem fog többé üzletet kötni Amerikával!”^[119]

A verbális agresszió, ami Donald Trumpnak is felróható, elnémítja az embereket, kitaszítja őket az információs térből, és még jobban csökkenti benne a hangok és vélemények mennyiségét. Ennek ellenére veszélyesen alábecsülik a nyelvezet információs térbeli eldurvulásának hatását – a politika is.

Ha egyszer elhangzanak az információs térben, még ártalmatlan szavak is felháborodott és ellenséges visszavágásokat válthatnak ki, ha olyan befogadóra találnak, akit félelmek és traumák gyötörnek. Ha a „pók” szó összetalálkozik egy fóbiával, vagy a „Bundeswehr” szó poszttraumatikus stressz tüneteit váltja ki, érdemes előre felhívni a címzett figyelmét, hogy a közleményben bizonyos ingerszavak fognak elhangzani, és tartalmi figyelmeztetést intézni hozzá.

Egy tendencia, amely kivált a Twitteren manifesztálódik világosan, nálunk is egyre jobban kihat a fizikai életre: gyakorlatilag minden egyes szó képes rossz érzéseket kiváltani, olyannyira, hogy a jövőben a nyelv számos szavának használatát kerülni leszünk kénytelenek. Bécs önkormányzata egyelőre nem nyúl a 2. kerületi „Negerlegasse” (Negerle utca), a Große Mohrengasse” (Nagy mór utca) és a „Kleine Mohrengasse” (Kis mór utca) elnevezéshez. Amerikai egyetemek azonban már átalakítják kötelezőolvasmány-listájukat. A nyelvi érzelemkeltésnek fatális következményei vannak, a jövőben ugyanis egy-egy nyelv számos

szavát nagy ívben kerülnünk kell majd. Ovidiust, Virginia Woolfot és Shakespeare-t tartalmi figyelmeztetéssel fogják ellátni. Máshol verseket festenek le homlokzatokon, szavakat csak részleteikben írnak ki: szxlis rszk. Ha már átfogalmazások megváltoztatják az emberek gondolkodását, akkor a nyelv lerövidítése a gondolkodás lerövidülését vonja maga után. Nhz lsz gndlkdn.

A nyelv, mint ez belátható, a jövőben még inkább elszegényedik, azért is, mert az emberek egyre gyakrabban beszélnek majd gépekkel, ám a gépek jelentéstani tekintetben (még) nem oly sokoldalúak, mint egy ember. Azonban már Ludwig Wittgenstein megállapította, hogy: „Nyelvem határai a világom határai”. Majd még meglátjuk, nem jár-e súlyos következményekkel, hogy mindannyian ennyire magától értetődően vesszük tudomásul a nyelv, az igazság és az értelem hanyatlását. Ám ahelyett, hogy határozottan elköteleznénk magunkat a jobb nyelvi képzés mellett, a politikában poszttextuális kommunikációra akarnak berendezkedni a jövőben. Komolyan fontolgatják, hogy engednek az infantilizálódásnak, és komplex politikai tartalmakat vizuális formában közvetítenek. „A választási eredmény XXX!” És az mégis milyen? Őrült vicces? Meggyőző? Rémes? Nem lehet nem meghallani? Logikai hiba, ha a politika felelősei abból indulnak ki, hogy a nyelvet mellőzve, pusztán képekkel is lehetséges értelmesen érvelni, és úgy tesznek, mintha a nyelv fejlődése, valamint az írásnak és az olvasásnak a könyvnyomtatás feltalálása nyomán bekövetkezett elterjedése semmilyen módon nem függene össze a Homo sapiens ismereteinek újkori, robbanásszerű megsokasodásával.

Egy biztos: a kommunikáció tálibosítása nagyon kapóra jön az olyan tömegvezetőnek, aki mesteri alkalmazója a nyelvi demagógiának. Ez esetben nincs jelentősége, hogy a digitális társadalmi tömeget kívülről egy harmadik állam trolljai, vagy pedig belső szereplők viszik tévútra. Az ér el eredményt, aki érvényesíteni tudja a hatalmát, akár a hazugság vagy a provokáció eszközeivel is. Mivel azonban a globalizáció korában – hangzik az ellenérv –, az információ gyorsan terjed, és (még) mindenütt lehívható, fikciót és világnézetet aligha lehet fenntartani hosszú távon. Ez legalább egy reménysugár...

Hogyan tovább?

A médiaoffenzíva után

Határparanoia, összeesküvés-elméletek, bevándorlók és iszlám elleni uszítás, Hillary Clinton elleni támadások, Donald Trump támogatása – mindez orosz eredetű politikai reklámként jelent meg,^[120] és a Facebook egyik értékelése szerint 126 millió amerikai választóhoz jutott el.^[121] Maguk a szponzorált Facebook-profilok nevei ártalmatlannak tűnnek. A Heart of Texas, a Born Liberal, az Army of Jesus, az LGBT United, a Black Matters vagy Blacktivist nem ébreszt gyanút amerikai célcsoportjaikban.

Nehezen állapítható meg, hogy a digitális információs térben folyó felforgató médiatevékenység sikeres-e, és legfeljebb csak spekuláció tárgya. De még ha abból indulunk is ki, hogy a szubverzív cselekedet előidézte a kívánt társadalmi változásokat, és csakugyan változás következett be az uralmi formában, a felfor-

gató szembesül a kérdéssel: végül is mit ért el szubverzív akciójával? Mi jön a felbomlási folyamat és az érzelmi fellángolás után, amit az online platformok váltottak ki? Hová helyeződött át a hatalom? Képes-e kontrollálni az új hatalmi viszonyokat a szubverzív szereplő? Van-e kapcsolat közte és a hatalom új birtokosa közt?

A felforgató cselekedetet nem szükségképpen a kívánt állapot követi. Az az állapot ugyanis, amelyben egy ilyen nagy mértékben hálózatba kapcsolt szereplőkből álló bonyolult társadalom végül ismét nyugvópontra jut, sohasem látható előre, a hatás nem tervezhető. Az elképzelhető kimenetek egészen különbözők lehetnek: kezdve azon, hogy egy bizonyos kormány kényszerítette érzi magát egy másik cselekvésre, azon át, hogy egy ország meggyengül, egészen addig, hogy hatalmi vákuum jön létre. Ezt roppant szemléletesen példázza Oroszország beavatkozása a 2106-os amerikai elnökválasztásokba. Ha csakugyan ok-okozati összefüggés volt a beavatkozásuk és aközött, hogy Donald Trumpot megválasztották, Oroszország alighanem akkor sem egészen azt az amerikai elnököt kapta, akit elképzelt magának.

Az oroszok már két évvel Trump megválasztása után igen rossz véleménnyel voltak az Egyesült Államokról: már csak 19 százalékuk volt pozitív véleménnyel Trumpról, méghozzá ahhoz képest, hogy ez a szám 2017-ben 53 százalék volt, bármilyen kitartóan támadta is az elnök a *Russiagate*-ügyben nyomozó különleges ügyészt.^[122] Oroszország feszültségektől mentes kapcsolatokat szeretett volna Amerikával, helyette azonban

olyan viszony jött létre, amely csak új mélypontokat és visszaeséseket hozott, hatalomra pedig olyan elnök került, aki növeli a katonai kiadásokat, és új szankciókkal sújtja Oroszországot.

A szubverziós jellegű „arab tavasz” szintén máshogyan alakult, mint ahogyan a polgárok elképzelték. A 2011-es év a Közel-Kelet számára a tiltakozás időszakává vált. Az emberek Tunéziától Bahreinig mindenütt az újrakezdés eufóriájával fertőzték meg egymást, és szembefordultak diktatórikus rezsimjeikkel – minden egyes országban más-más politikai eredménnyel. E folyamatok mindegyikében közös volt, hogy a forradalmárok online platformokon találtak egymásra, ezeken koordinálták és szervezték akcióikat. Amikor azonban a rezsimjeikben csalódottak végül az utcákon találkoztak össze, az online hálózatok hatalma gyorsan elenyészett. Ahol sikerült a kormányokat leváltani, a lakosság nem volt képes betölteni a létrejött hatalmi vákuumot.

Egyiptomban a Muszlim Testvériség volt, amely a Tahrir téri forradalomból hasznot húzott. Már az arab tavasz előtt politikailag szervezettek voltak, és gyorsan képesek voltak elfoglalni a kormány hivatalukból elkergetett munkatársainak posztjait. Annak, hogy megszerezték a hatalmat, nem sok köze volt a tiltakozó tömegek demokratikus képviseléséhez. Uralmuk nem is tartott sokáig: a kormányzást ismét magukhoz ragadták a fegyveres erők. Líbia mint állam működésképtelenné vált, miután az „akarók koalíciója” elűzte államfői posztjáról Moamer el-Kadhafit. A líbiaiak még ma is várják, hogy az amerikaiak, ígéretükhöz híven, segítsenek nekik létrehozni egy új és stabil kormányzatot. Szíria esetében a szubverzió katonai beavatkozást

idézett elő, valamint az ország polgárainak, illetve ezek helyettesítőinek egy alig átlátható háborúját. Csak Tunézia alakult át valamelyest stabil demokráciává. A szubverzió bizonytalanságai ezért többet követelnek meg, mint pusztán médiamunkát. A szubverzióknak folyamatosan egyengetnie kell a megcélzott áttörés útját, míg tartósan el nem éri stratégiai céljait.

A célországbeli szubverzív tevékenység sikerét követően az ellenséges országnak nem kell feltétlenül arra törekednie, hogy fenntartsa a célcsoportja koherenciáját is. Ha Vlagyimir Putyin Oroszországa helyre akarja állítani régi nagyságát a cári birodalom vagy a világhatalomnak számító Szovjetunió mintájára, és hatalmát rövid idő alatt be akarja betonozni, az orosz elnök felforgató stratégiája már akkor bejön, ha a világ elhiszi, hogy Oroszország újonnan megerősödött nagyhatalomként tért vissza a világ színpadára, mert rendelkezik azzal a hatalommal, hogy meghatározza egy választás kimenetelét egy demokratikus országban.

Oroszország csekély gazdasági erejét nézve azonban ez igen távol áll a valóságtól – szokták ellenvetni.^[123] Lehet, hogy Oroszországnak megvannak a gyengéi, de el kell ismerni: külpolitikailag nem sikertelen. Hatalma megszilárdításához Vlagyimir Putyinnak éppen a nyugati demokráciák struktúrája, társadalmaik fragmentáltsága, meggyőződésrendszereiknek és ideológiáiknak sokrétűsége jön igencsak kapóra. Hibrid akciókkal – amelyek „kis zöld emberek”, vagyis felségjelzés nélküli katonák analóg hadműveleteit is magukba foglalják – Moszkva megkaparintotta a Krímet, Kelet-Ukrajnában pedig elindított egy alacsony

intenzitású, se kezdete, se vége háborút. Logikai bombák, azaz kártékony programok telepítésével a Kreml még nyugatabbra eső infrastruktúrák elleni támadásokat készített elő és tesztelt, idegen kormányok szervereit támadta meg, fedett online kémkedés útján nyugati választási kampánystratégiákról szerzett információt, nyílt informatikai műveletekkel, például bizalmas információk közzétételével és nyugati államok nyugati platformok felhasználásával történő bomlasztásával dezinformációs tevékenységet folytatott. A hibrid eljárások tökéletes összhangban vannak az orosz fegyverarzenál áttekinthetetlen megújulásával, a nukleáris leszerelési egyezmények semmibevételével, és a jövő superhatalmával, Kínával folytatott katonai partneri viszonyal. Mindent együttvéve az összes eszköz jól szolgálja a fölénk rendelt célt. Oroszország kisebb szomszédai fenyegetve érzik magukat a hatalmas szomszédtól, a gazdaságilag és politikailag nagyobb súlyú országok pedig nem egységesek abban, hogy miként alakítsák Oroszország-politikájukat a jövőben. Egykori ellenfeleinek bizonytalanságát és megosztottságát Moszkva feltétlenül sikernek könyvelheti el.

„Az igazi hatalom, hogy azt ne mondjam, a félelem.”^[124] „A félelem erős. (...) »Tagadnod, tagadnod és ismét csak tagadnod kell (...). Ha elismeresz valamit vagy bűnösnek vallod magad, halott vagy. (...) Mindent tagadnod kell, amit csak mondanak rólad. Soha ne ismerj be semmit.«”^[125] Ezek nem Vlagyimir Putyin szavai – Donald Trump az, aki efféléket ismételget.

„Teljesen rendben van, ha szomszédaink egy kicsit félnek Oroszországtól. Ha tartanak tőlünk – az jó!”, idézi ezzel szem-

ben Wolfgang Ischinger az egykori orosz külügyminiszter-helyettest, Georgij Mamjedovot.^[126] Egészen úgy hangzik, mintha a diplomata Ischinger bölcs megfontolásból választotta volna az orosz külügyér szavainak ezt a defenzív fordítását. A félelem ugyanis a demokrácia bomlási jelenségeinek kiváltója, amint ezt ma a liberális társadalmakban megfigyelhetjük. A félelem elbizonytalanít és idegessé tesz. A félelem hivatkozási alappá lesz a szabadság korlátozásainak elfogadására, ugyanis – tévesen – azt feltételezzük, hogy biztonságunk csak így növelhető. A félelemmel azonban csak több bizalmat lehet szembeszegezni. Agresszív szavak, provokatív képek és eltúlzott gesztusok viszont nem teremtenek bizalmat.

[HÁROM]

Fegyverkezési verseny a mesterséges intelligencia területén

A mesterséges intelligencia a jövő nemcsak Oroszország, hanem az egész emberiség számára. Aki ennek a fejlődésnek az élén halad, a világ ura lesz. (Vlagyimir Putyin)

Késő délelőtt cseng a telefon. A hívó egy londoni munkaerő-közvetítő. Megbízója, mint mondja, olyasvalakit keres, aki szakértője a statisztikai következtetésnek és Markov-féle döntési folyamatoknak a mesterséges intelligenciával kapcsolatban. Egy ilyen specialistának, ha tapasztalt, hajlandók magas, hat számjegyű éves fizetést biztosítani. Egészen pontosan 700 ezer dollárt. A hívott német matematikus technológiai specializációja pedig pontosan megfelel az ügyfél elképzeléseinek...

– Milyen iparágban tevékenykedik az önök ügyfele? – érdeklődött a matematikus a brit személyzeti tanácsadótól.

– Játékszoftvereket gyárt – feleli az.

Régóta nem titok, hogy néhány éve nagy pénzeket fizetnek a mesterséges intelligencia specialistáinak. A fiatal, frissen vég-

zett, megfelelő tapasztalatokkal rendelkező diplomások évi 300 és 500 ezer dollár közti fizetésekért kelnek el,^[1] legalábbis az angol nyelvű országokban. Az amerikai OpenAI közhasznú szervezet évi kétmillió dollár körül fizet csúcskutatóinak.^[2] Ha meg eladó egy startup cég, amely a mesterséges intelligenciát maga fejleszti, és nemcsak nyilvánosan hozzáférhető, olcsó késztermékeket használ, vételárát az ott dolgozó mesterségesintelligencia-szakértőinek száma is meghatározza. A vevők fejenként öt-tízmillió dollárt is kifizetnek, hogy biztosítsák maguknak a know-how-t, amelynek a világszerte kevés szakember a birtokában van.^[3]

Csak hogy a matematikus a legjobb szándékkal sem tudja elképzelni, mire használhatnák a Londonban épp most nyilvánvalóan oly keresett technológiákat éppen egy játékgyártónál. Vajon miféle igen bonyolult, de kötött szabályokat követő játékban lehetnek nem megfigyelhető, látens változók, amelyeknek az állapotát meg kellene becsülni?

A személyzeti tanácsadó rövid eszmecsere után feltárja a lapjait.

Az ügyfél a Pentagon, mondja.

– Most már értem – feleli a matematikus. – Az ügyfél az amerikai fegyveres erők egy fedőcége – stratégiai *maszkirovka* [titkosszolgálati játszma fedett identitásokkal] folyik, amerikai módi szerint.

Nem mondhatnánk, veti ellen a munkaerő-közvetítő, az ügyfél valóban játékszoftvereket fejleszt, csak egyetlen részlege dolgozik a védelmi minisztérium számára.

Az amerikai védelmi kutatásokba mintha bőségszaruból ömlenének a dollárok. A tehetségek utáni vadászat során nagyvonalúan eltekintenek az *America First* és az *America Alone* jelszavaktól, a keresést időközben az egész földkerekségre kiterjesztették. És úgy tűnik, az olyan apró kellemetlenség, mint az európai vendégmunkások munkavállalási engedélyének a Brexit következtében való bevonása, csak a szolgáltatóiparban dolgozó lengyel munkaerő számára jelent leküzdhetetlen akadályt munkaviszony létesítésekor Nagy-Britanniában.

A matematikusnak fenntartásai vannak, s először pontos információkat akar szerezni az ügyfélről. Az ügyfél kedvező anyagi helyzete stabil: 500 millió dollárnyi saját tőkével rendelkezik, ami meglehetősen pénzügyi biztonságot teremt. Ennek ellenére meglepő, hogy a céget a japán Softbank Group finanszírozza, amelynek alapítója, Szon Maszajosi Japán leggazdagabb emberének számít. A Softbank Group-hoz tartozik a Softbank Vision Fund nevű befektetési vállalat: egy 100 milliárd dolláros működőtőkéjű befektetési alap, amely ezt a pénzt jövőbeli technológiákba, például a mesterséges intelligenciába fekteti. A tőke csaknem felét, 45 milliárd dollárt Szaúdi-Arábia adja.

Ez gyanús, állapítja meg a matematikus. Lehetséges, hogy külföldi államok kerülőúton, cégekbe való közvetlen befektetéssel akarnak hozzáférést szerezni olyan technológiákhoz, amelyek fegyverkezési szempontból érdekesek? Elképzelhető, hogy egy superhatalom védelmi minisztériuma olyan fedőcéget működtet valamely baráti országban, amelyet egy harmadik államban bejegyzett befektetési alap támogat, amely alap viszont Sza-

údi-Arábiából, tehát egy olyan államból szerez pénzt, amely a terrorizmus támogatásáról híresült el? Vajon ki fér hozzá végül is a technológiákhoz, amelyek a 21. században háborúról és békéről dönthetnek – államok és zsoldoscégek efféle hálózatában?

– Tudni akarom, melyik kormánynak dolgozom – mondja a matematikus a munkaerő-közvetítőnek.

Az soha többé nem jelentkezik nála.

Háború harcosok nélkül?

A helyettesítő háborúkról gondolkodva az ember feltétlenül beleütközik a mesterséges intelligenciába és a robotikába: együttesen képesek helyettesíteni a humán harcost. Lelkes hívei ezért a „harcosok nélküli háború” narratíváját terjesztik – , olyan csataterőről beszélnek, ahol már csak személyzet nélküli gép küzd személyzet nélküli gép ellen.^[4]

A kognitív, tehát olyan gépről szóló narratíva, amely hamarosan minden embert kiszorít majd, a gazdaságban is makacsul tartja magát. Pedig nem sok olyan gazdasági modell létezik, amelyben a mesterséges intelligencia a forgalom szempontjából relevánssá válik, és jövedelmezően alkalmazható. A legnagyobb vállalkozói hasznót a mesterséges intelligencia két üzemi funkciójában hozza, a reklámban és az értékesítésben, továbbá termelési és szállítási folyamatoknak jobb menedzselésében az értékteremtési láncban, más szóval a kiskereskedelemben és a logisztikában.^[5] Ezek azok a területek, ahol a technológia-eladók

és tehetségeik koncentrálnak. Noha a technológiai koncepciók a gazdaságban jóval kevésbé érdekesek, mint katonai kontextusban, ráadásul kutatásigényesek, a gazdaságban legalább pénzeső hullik.

Ezért van, hogy azoknak a kormányoknak, amelyek egyetlen szuperhatalmat sem képviselnek, nehéz a dolguk, ha tehetséges technológusokat akarnak átcsábítani a gazdaságból. Pedig az állami kutatólaborokban dolgozó úttörők voltak azok, akik a mesterséges intelligencia alapjait lerakták. Katonai rendszerekben az általunk ma ismert mesterséges intelligencia elődeit már több mint két évtizede alkalmazzák. Újnak tehát nem új, és nem is a Google találta fel. A mesterséges intelligencia se nem fegyver, se nem egyedi technológia, hanem egy átfogó koncepció, amely igényes matematikai elméleteket és különböző technikai eszközöket ötvöz különböző alkalmazási kontextusokban, új gépi képességek létrehozása céljából.

„A pusztító autonóm fegyverrendszerek számára a mesterséges intelligencia kulcstechnológiákból álló építőszekrényt tart készenlétben”, állapítja meg helyesen a svájci Jean-Marc Rickli. [6] A mesterséges intelligencia egyaránt lehet egy fegyver hordozóplatformja és maga a fegyver is. Ennek az a feltétele, hogy mindkettő rendelkezze a környezet értékelésének képességével, mielőtt meghozza az önálló döntést egy objektum célbavételéről és semlegesítéséről. A mesterséges intelligencia katonai haszna ezért továbbra is az „érzékelni és hatni” összjátékában rejlik. [7] A katonai zsargonban szerepel a *Situational Aware-*

ness/Understanding és Battle Management (szituációtudatos-ság/megértés és harcirányítás) is.

Ahhoz, hogy egy intelligens gép érzékelje környezetét, nagy adatmennyiségeket valós idejű helyzetképekké kell egyesítenie. Kezelő nélküli platformokra telepített, radioaktív, biológiai vagy vegyi harcanyagokat érzékelő szenzorok például szennyezett környezetben nagy mennyiségű adatot gyűjthetnek, dolgozhatnak fel, és vizsgálhatnak valószínűség szempontjából. Szenzor-készletüket ezután optimalizálva egy veszélyforrásra irányítják – e folyamatot nevezik *sensor cueing*nak –, és cselekvési alternatívákat javasolnak, hogy a biztonsági erők intelligens döntéseket hozhassanak önmaguk védelmére.^[8] A mesterséges intelligenciának tehát nem az a feladata, hogy felváltsa, hanem épp ellenkezőleg, hogy támogassa az ember, aki így tájékozottabban és gyorsabban hozhatja meg döntéseit – ezt a fajta együttműködést nevezik ember–gép-kooperációnak is.

Nekünk azonban nem a *good bot* (jó robot), hanem a *bad bot* (rossz robot) okoz gondokat. Különösen félelmetesek az emberek számára az olyan mobil autonóm gépekkel dolgozó horror-foratókönyvek, ahol a gépek önállóan döntenek egy ember életéről vagy haláláról. „Being killed by a machine is the ultimate human indignity” – a legméltatlanabb dolog, ami egy emberrel történhet, hogy egy gép öli meg.^[9] Ez összecseng a méltóságteljes halál iránti igénnyel, amiről egészen más összefüggésben, nevezetesen az eutanáziával kapcsolatban vitatkoznak a társadalmak, de – s ez meglepő – a katona azon jogával is, hogy maga hozza meg a döntést, öljön-e. Bizonyos fokig a katona gyámság

alá kerül, ha az életről és halálról való döntést egy gép veszi ki a kezéből. Szuverenitása is csorbát szenved, szabadsága is korlátozódik, ha a jövőről többé nem ő maga, hanem egy tárgy dönt.

Ha tehát egy digitális szabotázs alkalmával a környezeti intelligenciát kártékony szoftverrel támadják, ez legfeljebb közvetett módon okozza emberek halálát. Amikor azonban egy gyilkos robot támad, az ember közvetlenül veszti el az életét. Ahogyan egy „rádiótávírányítású, pilóta nélküli berendezés”^[10] kategóriájába tartozó, személyzet nélküli repülő platform célzott légitámadása során. Ez lehet *Remotely Piloted Vehicle* (RPV, távírányítású jármű), vagy részben autonóm drón – amit nem látni és gyakran nem is hallani, de képes ölni.

A drónok támadása

Nicolás Maduro Moros, a venezuelai államelnök vitatott államfő. Újraválasztását, mint ez a 2018. május 20-i előrehozott választások alkalmával kitűnt, számos állam és az Európai Unió sem ismeri el. Maduro korrupt vezetőnek számít. Országát tönkretette, és csalárd módon megfosztotta a venezuelaiakat az ország gazdag olajforrásaiból származó bevételektől. A valutát leértékelték, az ország inflációs rátája a Nemzetközi Valutaalap szimbolikus becslése szerint több mint egymillió százalék.^[11] A természeti erőforrásokban gazdag ország lakói nap mint nap éheznek. 2018-ban a szegénység elől körülbelül két és félmillió venezuelai menekült a szomszédos államokba. Ez aránytalanul

nagy terheket ró Kolumbiára, Brazíliára és szomszédaikra, Perura meg Chilére, ezért agresszíven reagálnak a kétségbeesett emberek érkezésére, többek közt azért, mert ezek között az országok között is akadnak, amelyek nemzetközi segítségre szorulnak.

Madurónak sok az ellensége. A fegyveres erők vezérkara ennek ellenére felsorakozik mögötte, amikor 2018. augusztus 4-én egy parádén a Nemzeti Gárda több ezer tagja vonul el előtte. Hirtelen robbanások hallatszanak, Maduro és felesége – mindketten az elnöki emelvényen – az égre emelik tekintetüket. A katonák az utcán még alakzatban állnak, de aztán felbomlik a rend, pánik keríti hatalmába az egyenruhásokat, és átmenekülnek a Bolivar sugárútnak az elnöki tribünnel szemközti oldalára.^[12]

Az államelnök ellen két robbanóanyaggal megrakott drón intézett támadást, állt utóbb az esetről szóló egyik kommentárban. Egy drónt állítólag sikerült kiiktatni, annak magyarázatával azonban, hogy miképpen, Venezuela adós maradt. Mások kétségbe vonták, hogy dróntámadás történt, és azt állították, a detonációt egy közeli házban keletkezett gázömlés okozta.

Amennyiben valakik dróncsapást hajtottak végre, nem a caracasi volt az első eset, hogy személyzet nélküli repülőeszközöket állami intézmények vagy magas rangú politikusok közelébe irányítottak. 2011-ben egy 26 éves amerikaiit vádoltak meg azal, hogy robbanóanyagot szállító modellrepülőgépet akart a Pentagonba és a Capitoliumba juttatni.^[13] 2013-ban, Drezdában, egy választási rendezvényen Angela Merkelt egy kereskedelem-

ben kapható drón közelítette meg, hogy aztán a német kancellár előtt zuhanjon le: egy kalózpárt tagja irányította rádión, aki ezt tiltakozásnak szánta a civilek ellenőrzése ellen. Angela Merkel barátságosan rámosolygott a drónra. Bizonyára nem merült fel benne, hogy drónok embereket támadhatnak és ölhetnek meg. Számos polgártársa ebbe mindmáig ugyanilyen kevésbé gondolt bele.

Az emberek ember nélküli rendszerekkel való pótlásának eszméje éppoly kevésbé új, mint maga a mesterséges intelligencia. Az ember nélküli rendszerek – levegőben, vízen és földön is – már két évtized óta léteznek. Külföldi bevetéseiken az amerikai katonákat sok éve támogatják robotok álcázott robbanóeszközök felderítésével, illetve épületharcban. Az amerikaiak földi bázisokról repülő robotokat szoktak bevetni a terror elleni harcban.

Miközben a nemzetek leszerelési konferenciákon már autonóm robotokkal végrehajtott támadások forgatókönyveivel foglalkoznak, a *személyzet nélküli légijárművek (Unmanned Aerial Vehicles, UAV)* ma még távirányítottak és csak félig autonómok. A Global Hawkhoz hasonló felderítődrónok egészen az utazómagasságig távirányíthatók, mielőtt autonóm módon tevékenykednének, hogy csökkentsék elektromágneses kibocsátási profiljukat.

Tervezőiknek a robotika mellett csak akkor szükséges mesterséges intelligenciát alkalmazniuk, amikor a pilóta nélküli rendszerek nagy mértékű autonómiával kell idegen terepen mozogniuk. A robotika és a mesterséges intelligencia tehát nem

ugyanaz; a technológia két különböző fejlesztéséről van szó, amelyek azonban lassanként összenőnek.

Az autonóm harci drónok (*Unmanned Combat Aerial Vehicles*, UCAV) ma csak technológiademonstráló eszközökként léteznek, és még évekbe telik, míg megérnek az alkalmazásra. Mindenesetre komoly kutató- és konstrukciós munka folyik velük kapcsolatban. Nagy előrehaladást tett Nagy-Britannia, az ő Taranis lopakodó bombázójuk állítólag képes az önálló légi harcra. Utánuk következik Németország és Franciaország, ők 2019-ben láttak hozzá a maguk „majdani harci légi eszközeinek” (*Future Combat Air System*je, FCAS) a kifejlesztéséhez, és az USA a „légi erő együttműködési rendszerével” (*Airpower Combat Air System*), amelyen a Boeing dolgozik. „Légifölény újragondolva”, hangzik az amerikaiak marketingszlogenje. Még a fegyverrendszereknek is kell a reklám.

A dróntechnológia professzionálissá válása nem jelenti, hogy a kereskedelemben mindenki számára elérhető drónok mindössze ártalmatlan játékszerek volnának.

„Ez a technológia, amit a magánszektor számára fejlesztettek ki, szédületes sebességgel terjed – horizontálisan az egész földgolyón, vertikálisan pedig az állami szereplőktől a nem államiakig” – állítja Jean-Marc Rickli.^[14] „A hidegháború vége óta a Nyugat mindig rendelkezett légifölénnyel. Most azonban egyszer csak rájövünk: elvesztettük a légtér feletti harcászati ellenőrzést”.^[15]

Az amerikai légügyi felügyeleti hatóság szerint 2020-ban egyedül az USA-ban mintegy hétmillió drónt vásárolnak keres-

kedelmi és magánfelhasználásra.^[16] A hatóság ezért úgy döntött, nagyobb mértékben tekintetbe veszi a veszélyt, amit a drónok a légiforgalom számára jelentenek. A drónok csempésznek drogokat, pénzt és fegyvereket, de akár egész repülőtereket is megbéníthatnak – például a londoni Gatwicket vagy Heathrow-t –, ha a kifutópálya felett köröznek, és veszélyesen megközelítik az utasszállító repülőgépeket.

A drónok már csak azért is gyorsan terjednek, mert – ahogyan a digitalizáció során oly gyakran – előállítási áruk csökken, miközben rendszersaját funkcionalitásuk egyre jobb és sokrétűbb. Humán támadóhoz való hozzárendelésüket mindazonkon a helyeken, ahol birtoklásuk nincs törvényileg szabályozva, már az is megnehezíti, hogy hatótávolságuk elérje a tíz kilométert, és hogy drót nélküli kapcsolat révén küldjenek információkat drónpilótáiknak, akik a földön tartózkodnak. (Az azonosítási nehézségeket jól ismerjük a gépjárműtartással kapcsolatban.)

A technika mai színvonalán álló kereskedelmi drónok némi ügyességgel különféle módokon veszedelmessé tupírozhatók. „Az Amazonon vásárolt drónoknak átépíthető a kamerájuk, illetve kézigránát rögzíthető rájuk”, tájékoztat a biztonsági tanácsadó Rickli. „Vadonatúj módja ez annak, hogy a Nyugatot a háborúval szembesítsék.”^[17]

De nem csak az képzelhető el, hogy drónokat harceszközökkel szereljenek fel. Helyzetmeghatározó szoftverrel ellátva a kereskedelmi drónok bármely célszemélyt is nyomon követhetik, akire ráállítják őket. Ha elveszítik a kapcsolatot földi bázisukkal, működésbe lép szabályozott vészhelyzeti programjuk,

amely gondoskodik a drón biztonságos leszállásáról. A drón elleni elektronikus védekezést megnehezíti a hőalapú képalkotás, az infravörös kamerák és a *Frequency Hopping*, a frekvenciaugratásos szórt spektrumú hozzáférés – a kereskedelmi drónok eladói egyre professzionálisabb eszközökkel látják el portékájukat. Egyre több hasznos terhet vihetnek. Egy kínai gyártó, a JD.com az ország postája számára készít drónokat, amelyek egy tonnányi súly továbbítására képesek. Ez csomagok egész sokaságát jelenti – vagy 19 Hellfire rakétát. A kínai kormány „civil-katonai fúzióval”^[18] biztosítja, hogy a kereskedelmi technológia kettős felhasználásra, s ekképpen katonai célokra is alkalmas legyen.

Az autonóm harci drónok színre lépéséig eltelik még néhány év. Mindazonáltal önálló drónok mesterséges intelligencia által koordinált és vezérelt rajaival lesz dolgunk hosszú távon. Amerikai kutatások, amelyek keretében rovar nagyságú, szúnyoghoz hasonló mikrodrónok helyiségeket fésülnek át, embereket támadnak meg, és halálos méreganyagokat fecskendeznek beléjük, valóságos horror-forgatókönyvek, ellenük indult az *Állítsuk meg a gyilkos robotokat!* kampány. A mikrodrónok nagy veszélyt jelentenek, mert minden ma ismert felderítési módszer és radaralapú légtérelőrzés számára felfedezhetetlenek. A mikro-repülőgépeket a radarok nem képesek érzékelni, korai észlelésük tehát nem lehetséges.

A drónok elleni 200 egyedi intézkedésen kívül, amelyek legtöbbje a katonai védekezés körébe tartozik, és civilek egyáltalán nem is folyamodhatnak hozzájuk, nem létezik *egyetlen* hatásos

védekezési lehetőség, amivel egy dróntámadást el lehetne hárítani.^[19] Miközben a kereskedelmi kvadrokopter elhárítására a legjobb eszköznek a sörétes puska számít, használata civil kontextusban alapvetően: tilos. Résztöltetes lőszerrel drónok elleni alkalmazását engedélyezik, a résztöltetek azonban valahol föl-det érnek, ami újabb problémák előidézője. Az európai katonai kutatás ezért lázasan dolgozik drónok felfedezését és követését, illetve elhárítását célzó koncepciókon. Más nemzetek ugyanis, az USA-tól Oroszországon át Kínáig, fegyverkeznek. Már csak idő kérdése, mikor néznek szembe országok állig felfegyverzett drónokkal, amelyeket a gyilkos méhek viselkedésére treníroz-tak. Hacsak a kormányok meg nem egyeznek a katonai célú (részben) autonóm drónok tilalmában.

A támadás előtt: érzékelés

Nap mint nap olyan döntések sokaságát hozzuk, amelyeknek a kimenetele nagy mértékben bizonytalan. Vegyek-e elektromos meghajtású autót, ha ma még nem tudni, hogy nem mégis az üzemanyagcella lesz-e uralkodó meghajtás-technológia holnap? Legyünk-e szállítói egy svájci vállalatnak, amelynek főrésztvényese egy orosz oligarcha – kockáztatva, hogy a cég holnap nehéz pénzügyi helyzetbe kerül, mert az illető oligarchát felvették az amerikai szankciólistára?

A második gépkorszak gépei, amikor kognitív berendezések végeznek majd szellemi munkát, szintén igényelnek majd infor-

mációkat arról a környezetről, ahol működni fognak. Helyesen kell érzékelniük a helyzetet. Az önvezető autóknak fel kell mérniük a forgalmi szituációt, mielőtt fékeznének vagy gyorsítanak. Legyen szó autonóm fegyverekről vagy hordozóplatformokról, hiperszonikus repülőgépekről vagy drónokról – mindnek „tudnia” kell, mikor áll fenn az összeütközés veszélye egy akadállyal. Képesnek kell lenniük az ellenség felismerésére, besorolásra és azonosítására, mielőtt az látótávolságon belülre kerül.

Erre egy algoritmikusan létrehozott helyzetkép teszi képessé őket. A helyzet ismerete nélkül a 21. század intelligens gépei sem tudnak tájékozott döntéseket hozni. Katonai összefüggésben ezért különbséget tesznek az „érezni” és a „hatni” között, ami annyit jelent, hogy a katonai helyzetet az érzékelő rendszerek ismerik fel és ítélik meg, hatórendszereken viszont az erőhatást kifejtő, potenciálisan pusztító fegyvereket értjük. Szigorúan véve azonban aligha alkalmazhatók a modern hatórendszerek helyzetismeret nélkül; a két rendszerkategória szorosan kapcsolódik egymáshoz.

Az aktuális helyzet kiszámításához és leképzéséhez környezeti adatok tömegét kell összegyűjteni: a környezet megfigyelés tárgya. A megfigyelés infrastruktúrája ugyanaz, mint amit az emberek az egymás közti kommunikáció és kapcsolatteremtés céljából használnak.^[20] A környezet megfigyelése során szenzorok sokasága a legkülönbözőbb adatformátumokat küldi egy multiszenzor-adatfúziós szoftvernek. Az adatformátumok a mérési adatsoroktól a képeken vagy videókon át a szövegig terjed-

nek. Mármost, az adatok egyesítésének művészete abban rejlik, hogy ezt a heterogén, úgynevezett nem kommenzurábilis adatforrásokból származó adattömeget gépi eljárások aktuális helyzetképpé egyesítsék és ábrázolják, továbbá lehetőleg egy értelmező komponenssel is ellássák, amely az emberi megfigyelő számára érthetően megvilágítja, hogy a gép miért éppen erre a helyzetértékelésre jutott.

Mindazonáltal számos kihívás létezik gépi megismerés alkalmazásakor. A környezetből gyűjtött adatok gyakran rossz minőségűek. Némely környezet infrastruktúra-szegény:^[21] nincsen se áram, se rádiókapcsolat, amire számos szenzorhoz kell, hogy az összegyűjtött adatokat továbbíthassák egy központi adatfúziós szoftvernek. Sok adat hiányos, sőt esetleg hibás – már ha közösségi hálózatokról származó adatokat is fel akarunk használni a helyzetkép kialakításához. Az adatok többértelműek lehetnek, ha hiányzik vagy ellentmondásos a kontextus, vagy ha a megfigyelt környezet lassanként megváltoztatja a szabályait, azaz nem stacionárius.

Ehhez jön még, hogy nemcsak az ebben a pillanatban, aktuálisan éppen fennálló helyzetet kell számításba venni. Még sokkalta érdekesebb, hogy a helyzet a közeli jövőben – valószínűleg – hogyan alakul majd. Gyakori ugyanis, hogy már most rendelkezünk a jövőre vonatkozó, töredékes információkkal. Ma tudjuk, hogy a koronavírus-járvány miatt 2021-re elhalasztott, tokiói Nyári Olimpiai Játékok július 23-ától augusztus 8-áig zajlanak majd. Amit viszont ma még nem tudunk, az az, hogy hány érmet nyernek majd egyes országok versenyzői.

Aki tudja, hogy valószínűleg mi történhet, jobb döntéseket hozhat, mintha vaktában, „hasra ütésre” kellene döntenie. A 21. század kognitív gépeinél sincsen másként, mint nálunk, embereknel. Akárcsak mi, ők is ismeretekre szorulnak, s ahogyan nekünk, nekik is előrelátásra van szükségük. Ehhez adatokat szereznek, információkat dolgoznak fel, és kivárlják, míg meghozhatnak egy döntést. A gépek azonban ennek során nem csak szisztematikusabban és gyorsabban járnak el, mint az ember. Az emberek másként tesznek szert ismeretekre, mint a gépek, és nem csak környezetük adattömegének elemzése útján. Az emberek úgy is ismerethez jutnak, hogy ismerik és alkalmazzák környezetük modelljeit – például a normarendszereket –, és hogy képesek tisztán elméleti megfontolásokra is. Isaac Newton a gravitációs törvényét mindenféle adattömeg-analízis nélkül fogalmazta meg. Albert Einstein is *Big Data* nélkül állította fel relativitáselméletét.

Az Egyesült Államok mégis gépi megismerésre óhajt támaszkodni, hogy kiderítse ellenfelei katonai szándékait. A gépi ihletésű érzékelés egyik konkrét alkalmazása az ellenséges államok atomrakétáinak levadászása.^[22] Intelligens gépeknek kell előre feltételezniük, hogy az olyan nukleáris hatalmak, mint Észak-Korea vagy Irán, mikor szándékoznak nukleáris töltet továbbítására alkalmas hordozórakétákat indítani. A mobil kilövőállások állomáshelyének követése ugyancsak az ilyen rendszerek funkcióinak körébe tartozik. Ez azért nem magától értetődő, mert az amerikai fegyveres erők ily módon azzal próbálkozik, hogy intelligens gépek segítségével felfedje az ellenfél terveit.

*Plan recognition*nek nevezik az intelligens gépek e feladatát, aminek során a cél az, hogy előre megállapítsák az ellenség szándékait. Intellektuális és koncepcionális teljesítményben ez túltesz mindenen, amit a Szilícium-völgy civil technológiai gigászai valaha is kiagyaltak vagy megvalósítottak. Az ellenség pszichéjének egy ilyen algoritmikus helyzetképén pedig folyamatosan dolgoznia kell a Pentagonnak, mert nemcsak a fenyegetéskörnyezet változik folyamatosan és váratlanul, de mára az is ellenséggé válhat, aki tegnap még szövetséges volt. Még a katonai kutatólaboratóriumok számára is nagy kihívást jelent annak a kérdésnek a nem-stacionárius volta, hogy ki ellenség, és ki nem az.

Állítsuk meg a gyilkos robotokat!

Az intelligens gépek képesek arra, hogy környezetünk adataival – az élet minden területén keletkező adatokkal, illetve felmérésük és feldolgozásuk sebességével – bizonyos feladatok esetében jobban boldoguljanak, mint maga az ember. Képesek átnavigálni minket gyarapodó környezeti intelligenciánk dzsungelén, s ezt már mint intelligens asszisztensek teszik, olyan jól csengő néven, mint Siri, Alexa, Cortana vagy Google Assistant.

Ahol az intelligens gépek kényelmet biztosító segítőknek bizonyulnak, ritkán jelent problémát a technológia elfogadása az emberek számára, és közömbösen viselkednek olyan negatív mellékhatásokkal szemben, mint személyük megfigyelése, ami

szükségképpen elválaszthatatlan velejárója az okos gépi asszisztensnőnek.

Jóindulatúan viszonyulunk az intelligens katonai eszközökhöz is, amennyiben védelmi célokra alkalmazzák őket. A fegyveres erők már évtizedek óta használnak eljárásokat a kognitív rendszerek nagy építőkészletéből, ha ellenséges légi célpontok multifunkcionális radarokkal való észleléséről, azonosításáról és leküzdéséről van szó. Jóllehet az ilyen radarrendszerek emberi közreműködés nélkül felismerik, azonosítják légi célpontjait, hogy aztán átkapcsoljanak egy másik üzemmódba, kövessék őket és rendkívül pontos adatokkal szolgáljanak róluk (és ennek köszönhetően irányított repülő eszközök nagy találati pontossággal semlegesíteni tudják őket), a védelmi fegyverrendszerek (rész)autonómiája eddig sem a népesség, sem a politika körében nem váltott ki tiltakozást. Nyilvánvalóan nagyobb súllyal esik a latba a megkönnyebbülés, ha a honvédelem intelligens eszközei nagyobb biztonságot nyújtanak a polgárok számára. A „biztonságossá tétel” fázisában ugyanis, amikor minden politikai kérdést a biztonság – az adatbiztonság, közlekedésbiztonság, a munkahelyek biztonsága, a szociális védelem – fényében is megvitatnak, a biztonság egyaránt becses érték és gazdasági tényező is.

Azonban a támadófegyverek, mint például a Taurus bunkerromboló, régóta ugyancsak részautonómiával rendelkeznek. Ez a levegő–föld cirkálórakéta, amelyet a bajorországi Schrobenhausen városkában fejlesztettek ki és gyártanak – a müncheniek tudják, hogy ott folyik a helyi spárgatermesztés is –, olyan precí-

ziós fegyver, amely bunkereket, hidakat, leszállópályákat vagy kikötőben horgonyzó hajókat képes elpusztítani. „Okos” például a Taurusban a gyújtómechanizmusa, amely maga dönti el, mikor lép optimális időben működésbe, ha egy többszintes bunkerbe csapódik be. Mielőtt felrobban, számolja a szinteket és érzékeli az üres tereket.^[23]

Különösen nagy félelmet vált ki az a radikálisan új légi fenyegetés, amit a teljesen automatizált drónok jelentenek. Mivel az új fegyverzeti technológiák – korábban a lőpor vagy a maghasadás – bevezetése az emberi történelem során mindig több, nem pedig kevesebb háborús halottat követelt, államok egy csoportja az úgynevezett „killerrobotok” betiltására törekszik, ahogyan ezt 2019-ben, a genfi Állandó Leszerelési Értekezleten 28 állam szorgalmazta. A lépést persze Ausztrián és a pápai államon kívül eddig egyetlen európai ország sem támogatta.^[24] A tilalom szorgalmazóiként abból indulnak ki, hogy a legmodernebb technológiák bevetésekor is sok ember fog majd meghalni. A NATO egyik agytrösztje „hiperháborúnak” nevezi az ilyen háborút, amelyben a csatákat a mesterséges intelligencia, az automatikus vagy autonóm rendszerek döntenek el, de az ember sem fogja pusztán csak érdeklődve nézni a gépi ütközeteket.^[25]

Mindenesetre a német népesség átmeneti megnyugvására szolgálhat, hogy a 2018-as koalíciós szerződésében lefektették: „Elutasítjuk az olyan autonóm fegyvereket, amelyek nincsenek alávetve az emberi beavatkozásnak, és világszerte törvényen kívül akarjuk helyeztetni őket.”^[26]

Ezt a politikai feladatot igencsak szűkszavúan fogalmazták meg; az életet pusztító autonóm fegyverrendszerek (Letale Autonome Waffensysteme, LAWS) törvényen kívül helyezésére vonatkozik, és attól akarja megszabadítani az embereket, hogy konfliktus esetén a gyilkolással kapcsolatos döntést kizárólagosan át lehessen engedni egy gépnek és pusztítóalgorithmusának. A gyilkolás végső felelősségét mindig egy embernek kell vállalnia – a szöveg megfogalmazóinak törekvése szerint.

Aki ez utóbbit szó szerint veszi, annak azután semmiféle kifogása nem lehet az autonóm fegyverrendszerek (Autonome Waffensysteme, AWS) ellen, amíg ezek nem halálos hatásúak, és csak más autonóm gépek támadását állítják meg. Ha egy államot LAWS-támadás ér, autonóm fegyverrendszere anti-LAWS-AWS-ként elfoghatja az ellenséges LAWS-t.

A LAWS körüli vitába Tobias Vestner nemzetközi jogász, aki a genfi Biztonságpolitikai Központ „Biztonság és Jog program”-ját vezeti, azzal a jogpozitivistá érvel kapcsolódik be, hogy sem a „nemzetközi hadijog, sem a nemzetközi humanitárius jog, vagy az emberi jogok” nem tartalmazzak előírást – sőt egy ilyen előírásnak még a szellemét sem – arra nézve, „hogyan ember [kell, hogy legyen], aki egy embert megöl”.^[27] Hogy a gyilkolásra miként kerül sor, továbbra is az államok, a hadviselő felek hatáskörébe tartozik. A lényeg mindössze annyi, hogy a gyilkolás ne ütközzék a nemzetközi jogba.

„Gyilkoljunk-e civileket vagy sem? Végrehajthatunk-e *targeted killinget* [célszemély kiiktatása], vagy sem? És mi a helyzet az okozott járulékos veszteségekkel?”^[28] – mindezek olyan kér-

dések, amelyeket a nemzetközi jogi előírások fényében kell mérlegelni.

Alapjában véve a LAWS esetében hasonló jogi és erkölcsi kérdések vetődnek fel, mint az autonóm gépkocsikkal kapcsolatban, állapítja meg Wolfgang Koch, a bonni FKIE (Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie) professzora.

Wolfgang Koch területe a katonai mesterségesintelligencia-alkalmazások kutatása. Véleménye szerint „egy autonóm autó is fegyver.”^[29] Egy autonóm autó is kerülhet olyan helyzetekbe, amikor életről vagy halálról kell döntenie. A hasonlat metaforikusan értendő; az autonóm járműveket természetesen nem fegyvernek tervezték.

De vajon képes-e arra egy gép, egy autonóm autó vagy fegyverrendszer, hogy jogkonform vagy erkölcsös módon viselkedjen? Ezt a kérdést különösen azoknak az államoknak kell feltenniük maguknak nagyon komolyan, amelyeket demokratikusan kormányoznak, és ezért az emberről alkotott ama elképzelést képviselik, hogy az ember több mint a gép, ugyanis szuverén, és képes felelősségteljes cselekvésre. Ezért a mindennapi élet tárgyai felett áll, és speciális méltóság a sajátja – az emberi méltóság. Nemzetközi viszonylatban és háborús helyzetben ezt a méltóságát a humanitárius nemzetközi jog védi. A diktatórikus berendezkedésű államok mindazonáltal alighanem kevésbé érzik úgy, hogy köti őket a szuverén emberkép, és hogy az ember védelemre szorul. Speciálisan európai emberképünk számos más állam kultúrájától idegen.

Ez pedig következményekkel jár, mert a LAWS fejlődése új fegyverkezési versenyhez és a politika radikális formaváltásához vezethet. Egyfelől, az autoritárius állami vezetők esetleg könnyen kitérhetnek a LAWS-szal összefüggő jogi és etikai kérdések mérlegelése elől (2016-ban egyébként világszerte csak az összes állam mindössze 63 százaléka rendelkezett demokratikus legitimációval – erről a körülményről szívesen megfeledkezünk, amikor az Egyesült Nemzetekre, valamint a békével és a biztonsággal kapcsolat kapcsolatos megbízatására hagyatkozunk). Másfelől, a LAWS fejlődése tendál afelé, hogy ezek az eszközök olcsóbbak legyen a hagyományos vagy a nukleáris fegyverek előállításánál. Ez visszavezet bennünket ahhoz a megállapításhoz, hogy a digitalizáció elmozdulást idéz elő a globális hatalmi viszonyokban, és kis államokat is alkalmassá tehet a 21. század helyettesítő háborúira.

Összefoglalva: a jogi és etikai nehézségeken kívül létezik még egy további ok is a LAWS elutasítására: a mesterséges intelligencia terjedőben lévő technológiáinak nem szabad a stratégiai egyensúly eltolódásához vezetniük, és az elrettentés és a védekezés helyett nem kedvezhetnek a támadó magatartásnak. A nemzetközi jog keretrendszerének, amely megköveteli, hogy a vitát politikai úton, diplomáciai eszközökkel és tárgyalásokon, ne pedig katonai erővel rendezzék, érintetlennek kell maradnia, s továbbra is előnyt kell élveznie a katonai konfliktusokkal szemben. Becsvágyó szándék ez – a LAWS-ok ugyanis digitális rendszerek, s mint ilyenek, „szükségképpen” pusztítóak, és így mindörökre megváltoztatják a hadviselést.

Automatikus vagy autonóm?

Időközben a LAWS-szal kapcsolatos fegyverzetkorlátozási folyamat elakadt, a vitában részt vevő államok juttatták kátyúba: huzakodnak. Kapitális akadályt jelent a definíciós probléma, hogy mit is jelent tulajdonképpen az, hogy „autonóm”. És miben különbözik ez az „automatikustól”? A tilalomnak ugyanis csak az autonóm fegyverrendszerekre kell vonatkoznia. Ez utóbbiakat az amerikai védelmi minisztérium a következőképpen definiálja: Autonóm az a fegyverrendszer, „amely aktiválása után anélkül képes célok kiválasztására és támadására, hogy ebbe emberi kezelőnek kellene beavatkoznia. Ide tartoznak az emberek által felügyelt olyan autonóm fegyverrendszerek, amelyek lehetőséget nyújtanak a kezelő számára a fegyverrendszer működésének leállítására, amelyek azonban aktivizálásuk után további adatbevitel és utasítások nélkül ismét képesek céljaik kiválasztására és támadására.”^[30]

Az egyik tábor úgy tartja, hogy „teljesen autonóm fegyverrendszerek jelenleg még nem léteznek”,^[31] ezért még nem is szabályozottak.^[32] E véleményhez csatlakozik Michael Biontino, Németország korábbi képviselője a leszerelési konferencián: „Az autonóm fegyverek maguk végzik a célfelismerést, nem rendelkeznek tárolt cél-könyvtárral.”^[33]

Némileg leegyszerűsítve: azt mondja, hogy a *kill decision* (ölési döntés) nem az ember kezében van. Szerinte az ember a cél leküzdésének teljes folyamatát – a támadási cél kiválasztásától, megtalálásától, azonosításától, megfigyelésétől és követé-

sétől, a célok rangsorolásától és az aktív rendszer modulációjáig egészen a célok semlegesítéséig és az összes feladatig és akcióig, melyek ez után a *kill chain* (ölési láncolat) után következnek – egy gépre bízta. Az ember maga távol tartja magát tőle. Mivel azonban emberek azok, akik feltételezik, melyek lesznek a támadandó célok – és a katonai akció során gyakran lesz így, amikor a fegyveres erők összehangoltan járnak el –, a célok leküzdésének folyamata nem autonóm, hanem legfeljebb automatikus, érvelnek az Állandó Leszerelési Értekezleten. Mivel pedig az emberi felelősségnek a teljes átruházása egy intelligens gépre ma még nem adott, jelenleg a tiltása sem lehetséges. Végül is, mondják, ami nem létezik, azt nem lehet szabályozni.

E végkövetkeztetés okán persze fennáll annak a veszélye, hogy a nemzetközi közösség soha nem fog megegyezni a LAWS betiltásában, s attól kell tartanunk, hogy az *Állítsuk meg a gyilkos robotokat!* kezdeményezést csak fél szívvel képviselik. Nyilvánvalóan egyetlen ország sem akarja, hogy gátolja valami az új technológiák kutatásában és fejlesztésében. A mesterségesintelligencia-technológiában vezető szerepet játszó államok ezért blokkolják a LAWS-tilalmat. Németország és Franciaország köztes pozíciót foglal el, nem kötelező erejű magatartási kódexet javasolnak. Egyedül Kína kötelezte el magát a kezdeményezés mellett. Támogatja a tiltást, fenntartja azonban magának a LAWS kutatásának és fejlesztésének jogát.

Németországhoz hasonlóan az USA is igyekszik aláásni a kezdeményezést, a nyilvánosság előtt azonban leszögezi, hogy a

jövő katonai konfliktusaiban nem szándékozik bevetni valamilyen *terminátort*.

„Igyekszünk olyan mesterséges intelligenciával rendelkező rendszereket találni, amelyek képesek cselekvési opciókat összeállítani és kiválasztani a [kívánt] hatás érdekében”, mondja Robert Work, Barack Obama és Donald Trump védelmiminiszter-helyettese.^[34] Szerinte senki sem akar egy emberi intelligenciával összevethető mesterséges intelligenciát. Igaz ugyan, hogy egy ilyen gép önállóan döntene a *kill cycle* (ölési ciklus) autonóm végrehajtásáról, emberként azonban azzal kellene számolnunk, hogy a gép esetleg megtagadja, hogy bármiféle célpontot kiválasszon. Megtámadják a saját országát, mire az okos fegyverrendszer vitatkozni kezd arról, hogy van-e kedve egy elmentámadáshoz? Abszurd ötlet, de következetesen autonóm.

Politikai akarat hiányában fog az időnk.

„Igen, vitatkoznunk kell”, erősíti meg Tobias Vestner nemzetközi jogász. „Több információra van szükségünk. [Az Egyesült Nemzeteknél azonban] az a tipikus tárgyalási taktika, hogy azt mondják, nem, nem, még nem állunk készen... Ezen a módon haladékot lehet kierőszakolni, vizsgálatok sokaságára lehet megbízásokat adni, és mindenki boldog. Előbbre azonban nem jutunk.”^[35]

A gépek ugyanis már régóta kategorizálják az embert, még hozzá a hálózatait és a viselkedése alapján. Így már ma is könnyen egy-egy gép célpontjává válhatunk. A chicagói rendőrhatóságok például egy gépet alkalmaznak annak eldöntésére, ki az 500 legveszélyesebb potenciális bűnelkövető. A megfelelő lis-

tát egy előrelátó rendőri munka céljait szolgáló algoritmus, a *Predictive Policing* állítja össze. A vélelmezett veszélyes személyek ekképpen fokozott rendőri ellenőrzés alanyai lesznek. Többségük fiatal afroamerikai férfi. Ez vajon véletlen? Vagy talán valamiféle technológiai rasszizmus megnyilvánulása? Ezzel kapcsolatban hadd jegyezzük meg: mítosz, hogy az intelligens gépek tárgyilagosan és előítéletmentesen döntenek. Döntéseik mindig csak annyira jók, mint azoknak a nyers adatoknak a minősége, amelyek egy-egy gépi döntés alapjául szolgálnak.

Mindenesetre már csak egy kis lépés választ el bennünket attól a géptől, amelyik egyre nagyobb találati pontossággal működő arcfelismerő egységgel kombinálva – az ilyenek fejlesztésében a kínaiak járnak az élen – önmaga meghatározza, felismeri és aztán semlegesíti célpontját.

E fejlemény ismeretében hogyan mozdítható ki tetszhalott állapotából a LAWS-vita? Frank Sauer (Universität der Bundeswehr, München) hangsúlyozza: a LAWS-ok nem a jövő fegyverei, hiszen a védelmi fegyverek már régóta autonóm módon működnek, és azt javasolja, távolodjunk el az automatikus kontra autonóm dichotómiától.^[36] Azt javasolja, a küzdelmet ne magáról a technológiáról vívjuk, hanem „az autonóm funkciókkal rendelkező fegyverrendszerek használata során alkalmazott katonai gyakorlat”^[37] engedélyezéséről vagy tilalmáról. Frank Sauer ezt úgy érti, hogy inkább abba kellene belegondolnunk, hogy a (rész)autonómia a hadviselés miféle olyan új formáit teszi majd lehetővé, amelyek eddig így elképzelhetetlenek voltak, s hogy a nemzetközi jog szempontjából hogyan kell ezeket meg-

ítelnünk. Így nézve ugyanis már egy „buta” szárazföldi akna alkalmazását is a LAWS-vita tárgyává tehetnénk, hiszen teljesen önállóan „dönti el”, ki a célpontja.

Sauer megközelítése, mely szerint arról kellene vitatkozni, hogy az ilyen modern, intelligens fegyverek bevetésének miféle bevetési forgatókönyveit tiltsuk vagy engedélyezzük, rendelkezne egy előnnyel: azokat az államokat is odaültetné a tárgyalóasztalhoz, amelyek eddig elutasították a LAWS egyetemleges betiltását.

Összhangban a nemzetközi humanitárius joggal?

Még ha nemzetközileg nem találták is meg a módját, hogyan lehetne elejét venni egy új, a LAWS-ok terén folyó fegyverkezési versenynek, egy bizonyos: az államoknak az érvényes nemzetközi jog szerint egyébként sem szabad „egyszerűen csak úgy” új fegyverrendszereket létrehozniuk. A nemzetközi fegyveres konfliktusok áldozatairól szóló, 1949. augusztus 12-iki genfi egyezmény 1977-es, kiegészítő jegyzőkönyvének 36. cikkelye ugyanis már előre számításba veszi új fegyverrendszerek létrejöttét, amennyiben felszólítja az államokat: vizsgálják meg, vajon nem kell-e eleve tiltottnak számítania egy-egy új fegyvernek vagy módszernek. Ugyanis a LAWS-ok kutatása és fejlesztése sem jogi vákuumban történik. A LAWS-oknak is jogilag szabályozottnak kell lenniük. Ezen a módon akarja megakadályoz-

ni a nemzetközi közösség, hogy új fegyverrendszereket idő előtt alkalmazzanak.

Mindazonáltal az, hogy jogszerű voltuknak ez a mérlegelése végül milyen eredménnyel jár, továbbra is az egyes államokra van bízva. Természetesen léteznek megfontolások és követelmények az új fegyverek engedélyezésének kritikus ellenőrzését illetően.^[38] Ebben az összefüggésben anyagi-jogi segítséggel két témaegyüttessel szolgál. Először: az új fegyver nem eshet egy meglévő leszerelési egyezmény hatálya alá. Másodszor: összhangban kell állnia a nemzetközi humanitárius joggal.

Az embereknek a második követelmény okoz fejtörést. A LAWS-oknak is egyértelműen képeseknek kell lenniük arra, hogy különbséget tegyenek harcolók és nem harcolók közt – s ugyanígy harcoló, valamint a *hors de combat* (harcon kívüli) katonák között, akik már megadták magukat vagy megsebesültek. Meg kell kímélniük a civileket is.^[39] Ha nem különböztetnének meg katonait és civilt, hanem különbségtétel nélkül ölnének, potenciálisan háborús bűncselekménnyel volna dolgunk.^[40] Mivel azonban a gépi osztályozás és azonosítás statisztikai alapon működik, a pontatlanság a rendszer immanens része. A gép hozhat téves döntéseket, okozhat úgynevezett álpozitív téves riasztásokat, vagy áldozatául eshet álnegatív tévedéseknek.

A harcolók és nem harcolók megkülönböztetése manapság még egy ember számára is nehéz. Mi a teendő, ha egy harcoló nem ismerhető fel mint ilyen, mert egyenruha helyett civil öltözetet visel? És ha ráadásul még egy civil védőpajzs mögött is elszáncolja magát, és a melléhez szorítva egy gyereket tart? Ha ci-

vil helyettesítője egy katonának, ami manapság, a 21. század helyettesítő háborúiban gyakran megesik? Gondoljuk az Airbus-konzernnek egy olyan munkatársára, aki a Bundeswehr valamelyik katonája helyett egy katonai bevetés során drónt irányít, mivel közreműködött a kifejlesztésében, és jobban ismeri a rendszert a megrendelőnél. Hadviselő lesz-e ekképpen a civil, vagy sem? (A válasz egyébként igen, és hamarosan, a védekezéssel kapcsolatos kérdés kapcsán közelebbről is szemügyre vesszük majd.)

A LAWS-oknak képeseknek kellene lenniük arra, hogy a cél leküzdése előtti döntési ciklus során ki tudják értékelni, vajon elkerülhető-e civil személyek megsebesítése vagy megölése. Ezt a döntést nem könnyű meghozni, rendkívül bonyolult lehet, mert a gépnek a kontextust is számításba kell vennie. Szükség esetén arra is képesnek kell lennie, hogy egy támadást önállóan félbe szakítson.

Ugyanilyen helyzet elé állítva egy ember olyan fogalmakra támaszkodna, mint a „jóhiszeműség”, a *soft law* (nem kötelező erejű jogszabályok) és a *sensus communis* (közfelfogás). A filozófus Markus Gabriel „egységesített benyomásról”^[41] beszél, ami emberekben egy hétköznapi jelenettel kapcsolatban alakul ki. Ez nem ugyanaz, mint az adatsaláta, amit egyetlen képpé kell egyesíteni. És ismét felvetődik a kérdés: tud egy gép úgy gondolkodni, mint egy ember? Kell-e egyáltalán, hogy úgy gondolkodjon, mint egy ember?

A célok megkülönböztethetőségének kérdéséhez még egy igen fontos problematika társul. A számadási kötelezettségről

van szó. Ellentétben az autonóm autóközlekedéstől, aminek esetében szintén meg kellene határozni a felelősség viselőjét, a katonák ez ügyben mindig is egy lépéssel előbbre jártak. Aki egy fegyverrendszert alkalmaz: felelős. Más szóval, ha a Bundeswehr fegyverrendszereket vet be, amelyeket egy fegyvergyártó konszern állított elő, a felelősség az üzemeltetőt, tehát a Bundeswehrt terheli, azaz nem a gyártót és annak programozóit.

Csak hogy a LAWS esetében nem volna-e unfair egy humán parancsnokot felelőssé tenni azért, amit egy LAWS, amelyet másvalaki épített, háborús bűncselekményt követ el – akár szándékosan, konstrukciójából következően, vagy akár csak tévedésből is?

A nemzetközi jogászok itt bevezetik a bizonytalanság fogalmát: a LAWS-ok, mint mondtuk, statisztikai alapon működnek. Ez nem jelent mást, mint hogy bevetésük esetén valószínűsíthető hatással működnek. A valószínűség eloszlása hisztogramként ábrázolható, és hogy mennyire bizonyos a bevetés valószínű következménye, azt egy-egy LAWS-fejlesztői statisztikai tesztek segítségével vizsgálhatják, mielőtt a rendszert kiadnák a kezükből.

A bizonytalanság fogalma mellett létezik az előzetes kármegállapítás, a *predictive damage assessment* koncepciója is: ennek értelmében bevetés előtt egy kisegítő rendszer kijelzi a parancsnoknak, hogy a harceszköz valószínűleg milyen károkat okoz majd.

Ez azt jelenti, hogy a parancsnoknak, aki bevet egy LAWS-t, tudatában kell lennie, milyen hatásokat fejt ki a fegyver bizo-

nyos helyzetekben. Az ő számára előreláthatónak kell lennie a kimenetelnek – ami a civil lakosságra kifejtett hatást illeti. Amennyiben nem ismeri a valószínűsíthető következményeket, az eszköz szándékos vagy kissé könnyelmű alkalmazása jogellenes lenne.^[42]

Az ezzel kapcsolatos számadási kötelezettség azonban egyaránt maga után vonná az érvényes nemzetközi humanitárius jog és a büntetőjog kibővítését. Szükségesek volnának azonban a LAWS-ok szabványosított és gondos tesztjei is, amelyekre a parancsnok támaszkodhatna. Ameddig azonban a nemzetek meg nem egyeznek a killerrobotokkal kapcsolatban szükséges szabályokban, a LAWS-ok katasztrofális következményekkel járhatnak a világ lakosságára nézve.

Szigorúan titkos: az elektronikus harc

– Itt German Airforce Tornado 4300,^[43] vészhelyzetet kell jelentenem. Kapcsolja ki azonnal azt az izét!

Még a rádión keresztül is hallatszik, milyen ingerült a vadászbombázó pilótája. Ahelyett, hogy meredek légi manőverekkel közelharcot szimulálna a gyakorlóterület felett, ahogyan megbeszélték, próbálja nyugodt, stabil repülési helyzetbe hozni a Bundeswehr védelemtechnikai szolgálati helyének Tornado harci gépét.

– GAF 4300, roger, műszerzavar. Mi a szándéka?

– Kapcsolja már ki végre azt az átkozott radart!

A német fegyverüzem fehérre meszelt gyártó- és irodacsarnokai mögötti tágas, zöld területen lustán terül el a kánikulai hőség. Az irodák ablakaiban vakítóan tükröződik a ragyogó verőfény. A hosszúkás épületegyüttest egy aszfaltút választja el az átellenben fekvő rétektől.

A fegyveripari cég számára, amelyet a népnyelv csak „az erőd” néven emleget, a gyártó részleg melletti, tágas üzemi terület létszükséglet: itt, a saját területén teszteli a gyártó a katonai célú, új rendszereket, mielőtt továbbfejlesztené, vagy átadná őket a gyártó részlegnek. A munkatársak a külső területet a rendszerteszteken kívül üdítő ebédszünetek céljaira is igénybe veszik. „Kifutó” – így emlegetik a csarnokok mögötti zöldterületeket. Itt akár az új katonai technológia mellett is sétálghatnak. A kifejezetten e célra létesített parkolóhelyeken zöld álcázószínre festett, nyolctengelyes tehergépkocsik állnak: mobil platformok, rajtuk a légtérvédelmi radarantennák, az ellenséges repülőgépek, helikopterek és rakéták elhárításának eszközei. Nem lehet nem észre venni egy nagy, többfázisú antennát: egyenesen nyúlik a magasba szállító járműve alvázáról, az eget kémleli; egyaránt alkalmas légtérfelderítésre és arra, hogy célt jelöljön meg radarvezérlésű légelhárító rakéták számára, majd rávezesse őket.

Némi távolságra tőle egy teherautó áll, amelynek rakfelületére egy konténert telepítettek. A légvédelmi rendszer fontos elemét alkotja, mert – mint egy apró, külön irodában – a radarirányító számítógépet és az algoritmikus adatfúziót helyezték el benne. A többfázisú radart civilruhás emberek ebből a mobil fe-

dezékből irányítják. Erre a napra mindössze egyetlen tesztet irányoztak elő. Műveleti bevetésen egyenruhát és rohamsisakot viselnének.

Az egész bolygót radarberendezések mindenre kiterjedő hálózata borítja be sugárzó energiájával. A turisztikai célú repülőutak számának állandó növekedése a túlszűfolt légtérben radarok nélkül már elképzelhetetlen volna. A sugárzás kibocsátása az elektromágneses tartományban történik, azé a sugárzásé, ami mindig is magától értetődő módon vette körül az embert, hiszen a látható fény is az elektromágneses tartomány eleme. De már régóta újabb komponensek társulnak hozzá: a rádióhullámok, a mobilok és a televízió hullámai, mikrohullám, GPS, Bluetooth és WLAN – a láthatatlan sugárzó energia tere mindinkább megtelik és egyre zsűfoltabbá válik.^[44] Sok ember nem érti, amit nem lát. Csak az elektronikus hadviselés profijai visznek fényt a sötétségbe érzékelőrendszereikkel. Tudják, hogy a sugárzás, ami ebben a mennyiségben és teljesítménysűrűségben korábban nem létezett, ma aktív menedzselést igényel. Ez egyfelől annyit jelent, hogy a fontos berendezéseket védeni kell a zavaró hatásoktól, mert ha szabályozatlanul magas a sugárzási energia, a modern ember mindennapjai nem zajlanak zökkenőmentesen. Másfelől létezik az ellenkező előjelű kihívás is: miként befolyásolható vajon egy potenciális háborús ellenfél elektromágneses spektruma – saját hadműveletek számára? Aki a spektrumot uralja, stratégiai előnyre tesz szert. Az amerikaiak iraki vagy afganisztáni háborúja elképzelhetetlen lett volna

elektronikai hadviselés, illetve a nélkül, hogy uralták volna az elektromágneses spektrumot.

A többfázisú radarok, amelyet az amerikaiak már a múlt század nyolcvanas éveiben telepítettek repülőhordozókra, évtizedekig tartó fejlesztésük során különösen alkalmasnak bizonyultak, hogy a legkülönbözőbb feladatokat teljesítsék a zsúfolásig teli elektromágneses spektrumban. Polgári alkalmazásban a 21. században a mobilhírközlésben „okos antennaként” honosodott meg. Ám továbbra is a katonai alkalmazásban szolgál a legtöbb előnnyel. Nevezik csoportantennának is, több négyzetméteres területén különálló sugárforrások sokaságát rendezik sorokba és oszlopokba. Hogy minden egyes forrás a többitől függetlenül képes legyen sugárzási energia kibocsátására, mindegyiket egy számítógépes program vezérli. A számítógépes program változtatja a pulzálás frekvenciáját, a sugárzások közti időtartamot vagy a fősugár irányát. A radarelektronikusok ezt *beamforming*-nak (kb. nyalábirányítás) nevezik. Mivel a komputer a radar sugárzási energiáját és ezzel az antenna teljes viselkedési karakterisztikáját ezen a módon valós időben, mikroszekundumokon belül változtatja, a többfázisú radarok ismét csak kihívást jelentenek a potenciális támadó számára, nehezen lehet ugyanis zavarni vagy semlegesíteni.

Ezen a stratégián – ami a II. világháborúban az elektronikus hadviselés első megjelenéséhez vezetett – máig nem változott semmi. Annak idején a szövetséges haderők célul tűzték ki, hogy elektronikusan zavarják a tengelyhatalmak radarállásait, s ezzel a kommunikációjukat. A mai napig érvényes, hogy csak

az elektronikus hadviselés teszi lehetővé az egyidejű védekezést és támadást, ezért továbbra is rendkívüli stratégiai jelentőséggel bír.

Katonai összefüggésben a többfázisú radarokat standard módon egy olyan eljárás során alkalmazzák, amelyet a technológusok *pipelining*nek (futószalag-elv) neveznek. A légtérfigyeléssel, valamint a repülő célpontok felismerésével és követésével kapcsolatos műveletekre egymást követően kerül sor. Mielőtt a radar kereső üzemmódban, a légtér letapogatása során repülő objektumot fog be, az visszaveri a sugárzást, és jelként küldi vissza az antennára. Ekkor teszi a szoftver láthatóvá, ami az emberi szem előtt rejtve marad. Ezután a radarképanalízis iktatja ki az állandó jeleket. Az állandó jelek a megfigyelt térség fix pontjai, többek között épületek és terepalakzatok, amelyek nem mozognak, ezért különösebben nem érdeklik a légtérrel-ellenőrzést. A megmaradó jelet végül egy képernyőn, térképszerű látványként jelenítik meg. Ha a radar érdekes jelet fedezett fel, bekapcsolja a követő üzemmódot, a *trackert*, és elkezdi a repülő objektum útjának követését, sőt előrejelzését. Eközben a jelfeldolgozás mindig csak egy problémára koncentrál: vajon az érzékelt objektum barát vagy ellenség? Itt is a számítógép segíti a továbblépést. Egy osztályozó algoritmus megállapítja a felfedezett dolog típusát, s majd csak ez után következik a légijármű konkrét azonosítása.

A mobil alállomáson, ahol a többfázisú radar főszámítógépét elhelyezték, feszültséget vált ki, amikor a vadászpilóta vészhelyzetet jelent. A radartechnikus figyelmét összpontosítva ír a bil-

lentyúzenen, hogy átvegye a radar működése feletti irányítást, amelyet rövid időre egy mesterséges intelligenciának adott át.

– GAF 4300, roger. Radar lekapcsolva.

Három órával az esemény előtt a kutatásvezető, a mesterséges intelligenciával foglalkozó kutatóteam, a radartechnikus, a Tornado pilótája és a Bundeswehr egy fegyverrendszer-tisztje összejött az eligazítóhelyiségben, mivel a többfázisú radar egy egészen sajátos tesztje volt soron: a radar irányítását első alkalommal kellett átvennie mesterséges intelligenciának. A tesztnek azt kellett igazolnia, hogy el lehet térni a szigorú, folyamatos pipelining-eljárástól.

A szoftvermérnökök e célból intelligenssé alakították át a radar vezérlését. Egymástól elkülönítve modellezték a rendszer minden egyes összetevőjét, a keresés vezérlését, az azonosítást és a trackert, a főszámítógépet és a radarhardvert, amelyek attól kezdve autonóm, decentralizáltan működő szervezetként viselkedtek. Egy megosztott mesterséges intelligencia minden külön komponenst egy-egy zárt programkód-darabbal reprezentált, amely azonban rendelkezett azzal a tulajdonsággal, hogy aktívan kommunikált, illetve folytatott interakciókat a rendszer más összetevőivel. Az ismeretek cseréje azonban nem közvetlenül a komponensek közt folyt, hanem egy virtuális falitábla, a *blackboard* közbeiktatásával. Ez volt a radarrendszer központi idegrendszere. Ha a tracker követésre érdemes célt fedezett fel, az információt minden egység számára látható módon felírta a virtuális táblára. Az információ érdekes lehetett az azonosító komponens számára, amely leolvasta, hogy a tracker légiútvo-

nal-számításaiból magasabb rendű bizonyítékot nyerjen a légi jármű identitását illetően. Ezért aztán ha új információ jelent meg a táblán, minden komponens ismét feltette magának a kérdést: vajon hasznos-e számomra a másik információja annyira, hogy javítsam saját helyzetértékelésemet?

Az élőlénnel való összehasonlítás nem véletlen. Egy egymással interakciót folytató, autonóm elemekből álló rendszerkonstrukció révén a fegyverzeti üzem szoftvermérnökeinek mesterséges intelligencia segítségével sikerült egy addig statikus egységekből felépülő folyamatot komplex dinamikus rendszerre átalakítani. A programkód valósággal életre kelt. Noha az új konstrukció célja világos volt – a radarnak légiharc esetén képesnek kellett lennie rá, hogy a szokványos eljárásnál jóval gyorsabban azonosítson és figyelemmel kísérjen egy *air theatert* (légi hadszíntér), amelyen szűk térben pilóták százai harcolhatnak egymással –, láthatóan volt egy hátránya: rugalmassága a vártnál csekélyebbnek bizonyult, nem lehetett előre látni, hogyan viselkedik majd a mostantól komplex, dinamikus radarrendszer.

– Alezredes úr, egyetlenegy harci géppel kezdjük meg az intelligens radarvezérlés tesztjét. Az ön Tornadója szimulálja a légi célpontot. Délnyugati irányban nagyobb magasságba emelkedik, majd miközben lefelé ereszkedik, átrepül a tesztterület felett. A két első átrepülésre egyenes vonalban kerül sor. Ezután hajthat végre speciális légi manővereket vagy vehet fel egyéb repülési helyzeteket, úgy, ahogyan ezeket légiharcra való felkészülésként is gyakorolni szokta.

Az alezredes biccent.

– Mialatt a manőverét végrehajtja, a többfázisú radarunk erőteljesen érdeklődik majd ön iránt – magyarázott tovább a kutatásvezető –, ezért ön úgy manőverez majd, hogy a lehető legtovább visszatartsa a radart az ön ellenségként való azonosításától, illetve követésétől.

– Nem tudjuk azonban pontosan megmondani önnek, hogy a radar valójában miként viselkedik majd – tette hozzá a rendszerfejlesztő. – Mivel a radarrendszer minden egyes összetevője a többitől függetlenül tevékenykedik, és önállóan követ egy stratégiát, amely nem szükségképpen ugyanaz a problémamegoldó stratégia, mint a többi komponensé, nem tudjuk pontosan, hogyan jár el majd végül önnel kapcsolatban a rendszer egésze.

– Vagyis nem tudják, hogy a radarvezérlés végül milyen állapotba áll be? – firtatja a pilóta.

– Így van. Az is elképzelhető, hogy a radar egyáltalán nem önre fókuszál, mert egyes elemei nem jutnak el egy közös összestratégiáig – felelte a rendszerfejlesztő.

A kutatásvezető helyeslően bólintott. – Optimális esetben begyűjtjük és kiértékeljük a radar viselkedésének adatait, hogy megállapítsuk, jár-e katonai előnnyel az új design. Ez volna például a helyzet, ha az ön Tornadóját gyorsabban vagy könnyebben tudná követni, mint egy hagyományos tracker.

– Vagy ha az információnak a *blackboardon* való megjelenítése alkalmas arra, hogy azonnal igazolja a légi célpontok azonosításának érvényességét – teszi hozzá a rendszerfejlesztő. –

Mindenesetre egy hagyományos trackert gyorsan túlterhel, ha az égen nagyon sok dolog történik.

Az alezredes feláll a székéből: – Könnyű gyakorlat. Elkezdhetjük.

Az első két átrepülésnél a pilóta semmi feltűnőt nem észlel. Mialatt a földi team regisztrálja a Tornado közeledését, a gyakorlat a gép fedélzetén is a tervek szerint zajlik. A pilóta végrehajt két Immelmann-fordulót, majd támadást szimulál. A harmadik átrepülés során azonban kényes helyzet alakul ki. Egyszer csak váratlanul zavarni kezdi valami a terepkövető radarját. Mihelyt egy harci gép nagy sebességgel kis magasságon, egyenetlen terep felett száguld, a terepkövető radar segítségével történő navigáción múlik a pilóta épsége, élete. Az alezredes képernyőjén azonban már csak értelmezhetetlen jelzuhatag látszik.

Az alezredesen idegesség lesz úrrá, megpróbálja visszanyerni uralmát a gép felett, és irányt változtat. A radar sugárnyalábját azonban nem tudja lerázni. A fedélzeti számítógép még a többfázisú radartól közepes távolságra is eszeveszett dolgokat művel. A kockázatos légi manőverek, amelyeket néhány órával korábban az eligazítóhelyiségben megbeszéltek, most már túlságosan veszélyesek lennének. A harci gép helyzete csak az után válik ismét biztonságossá, hogy a pilóta rádión vészhelyzetet jelent.

– Kapcsolják le végre azt az átkozott radart!

– GAF 4300, roger. Radar lekapcsolva.

A kutatóteamet teljes meglepetésként érte a váratlan tapasztalat. Aki legfeljebb azzal számolt, hogy a radar engedelmesebb lesz, az a mesterséges intelligencia életbelépésekor az ellenkezőjéről győződhetett meg. Olyan erővel összpontosította a radar a sugárvezérlését a Tornadóra, hogy emiatt gyújtólencsehatás lépett fel. A radar – anélkül, hogy mérnökei és technikusai akarták volna, vagy közreműködtek volna – teljesen önállóan elektromágneses impulzushoz hasonló sugárzást hozott létre, és ezzel kockázatos módon megzavarta a harci gép érzékeny fedélzeti elektronikáját. A radar elektromágneses támadást intézett a vadászgép ellen: a pilóta, nehogy maga is életveszélybe kerüljön, megszakította repülési manőverét, stabil repülési helyzetbe hozta a gépét, és kérte a radar lekapcsolását. A radar ilyenképpen sikeresen destabilizálta a harci gépet, ami, ha nem gyakorlat zajlik, veszélyes helyzet lett volna. Először destabilizálni, aztán lelőni – valódi légi harcban ez lehetett volna az ellenfél taktikája. A kutatócsoport dinamikusabb célkövető algoritmus helyett egy elektronikus bombát fejlesztett ki, amelynek alkalmazása ugyanúgy a harci gép lezuhanásához vezethetett volna, mint ha rakétával lövik le. Önálló életre kelt tehát egy radar, amelyet mesterséges intelligencia vezérelt. Fejlesztői egyikében sem merült volna fel, hogy a rendszer saját hadviselési módszert fejleszthet ki.

– GAF 4300, fejezzük be. Akar még egy keveset csavarogni odafenn?

– Megyek és leszálok. GAF 4300.

– GAF 4300, rendben. Lépjen kapcsolatba a toronnyal a 122,1-en.

– 122,1... További szép napot. GAF 4300.

Régen volt már ez a „szép nap”: 1996 forró nyarán. Az akkori közreműködő német mérnökök egyike sem fejlesztette tovább az elektronikus bombát, sietve eltűnt a terv az asztalfiókban. Nem azért, mintha nem működött volna. Nem is azért, mert a geopolitikai helyzet a jelek szerint úgy megváltozott, hogy a fegyverkezési verseny és a hidegháború a múlté lett. Más volt az oka. Időközben a „kifutó” egy európai biztonsági szolgáltató konszerné lett, amely 2013-ban bejelentette az állomáshely bezárását. A cégegyesülések, vegyesvállalatok, átnevezések és részleges kivásárlások közbeeső zűrzavara során a britek egy trükkös húzással eltulajdonították a német fegyveripari cég radartechnológiáját – törvényesen ugyan, de Németországban gyakorlatilag észrevétlenül. Az egykori erődöt ma, csaknem huszonöt évvel később, ipari parkká alakították.

A németet kutatók csak azóta összpontosítanak ismét jobban a sugárzási energiára, hogy az elektromágneses spektrum olyan mértékben telítődik, hogy már alig tudja valaki elképzelni, milyen az, ha nem lehet mobil módon szörfözni, vásárolni, telefonálni és dolgozni. Nemrég óta ismét élénk vita folyik katonai tudományos körökben az elektronikai hadviselésről. Amióta egyre sebezhetőbb a társadalom, mert minden területen – a mobil dolgozástól az autonóm járműveken át a tárgyak-dolgok ipari internetéig – az elektromágneses spektrumra támaszkodik, Oroszország, Kína és az USA elektromágneses fegyverkezést

folytat, hogy biztosítsa stratégiai előnyét. Ami az európaiak számára első ránézésre joggal észszerűnek és kívánatosnak tűnt, nevezetesen a leszerelés a Varsói Szerződés bukását és a biztonsági követelményszint ezzel összefüggő csökkentését követően, keservesen megbosszulhatja még magát a 21. század helyettesítő háborúival kapcsolatban.

Az Achilles-sarok: az elektromágneses spektrum

Wolfgang Koch, a FKIE professzora biztos abban, hogy „a mesterséges intelligencia katonai alkalmazásai sokkal többet jelentenek »kilobotoknál«. „Személy szerint úgy hiszem, hogy a »kinetikus hatást«, ahogyan udvariasan mondani szoktuk, kevésbé uralja majd a mesterséges intelligencia, mint az »elektronikus hatást«. Az elektronikus hadviselés a cyberháború természetes kiegészítője, és igen nagy jelentőségre tesz majd szert.”^[45]

Digitalizáció nélkül a modern hadviselés nem képzelhető el. Az egyre több ember nélküli rendszer gyorsan és tartósan alakítja át a katonai műveleteket. A távvezérelt, személyzet nélküli rendszerek azonban rá vannak utalva a földi bázisukkal való rádióösszeköttetésre, ugyanígy az autonóm rendszerek is az elektromágneses sugárzásra. Szenzoraik azt veszik, ami körülöttük történik, távolság- és pozícióméréseket végeznek, hogy tudják, hol tartózkodnak. Valós idejű adatokra kell támaszkodniuk, amelyeket megszakítás és átviteli szünetek nélkül szerez-

nek, feldolgoznak és esetleg más rendszerekkel is megosztanak egy művelet során.

Kommunikációjuk és érzékelésük érdekében a fegyverrendszerek éppúgy kihasználják az elektromágneses spektrumot, mint mi, emberek, amikor okostelefonon telefonálunk, okos, drótnélküli vízórákat építünk be a házunkba, vagy majd ha egyszer autonóm autóval közlekedünk. Az elektromágneses spektrum nélkül nem volna lehetséges a mobil kommunikációnk. Ezért a katonai célú, hálózatba kapcsolt rendszerek mellett a mi civil környezeti intelligenciánk is különös védelemre szorul, és konfliktushelyzetben rendkívül veszélyeztetett. Az is konfliktushelyzet, amikor uralni akarják az elektromágneses spektrumot, illetve információs fölényre igyekeznek szert tenni.

Egy támadás megbénítaná az elektromágneses spektrumot, visszakatapultálná az életünket a 20. század kilencvenes éveibe. Egy ilyen támadás Koch professzor felfogása szerint kommunikációs infrastruktúránk elleni szabotázs volna, csak hogy immár nem hekkertámadások, vírusok vagy férgek alkalmazása útján – amelyek megbénítják a számítógépeket, ipari létesítményeket vagy az energiaellátást –, hanem egy ellenfél nagyfrekvenciájú sugarakkal végrehajtott „bombatámadása” formájában. Nem mi magunk „vakulnánk” meg, hanem környezeti intelligenciánk, mert már csak hamis információhoz juthatna – vagy egyáltalán semmilyenhez. Egy elektromágneses spektrum elleni támadás tehát nem az emberi érzékelést zavarná, hanem okos gépeinkét, amelyekre oly nagy mértékben támaszkodunk.

Elektronikus hadviselés azóta létezik, amióta a rádiótechnika bevonult a fegyveres erők kelléktárába. Azt azonban, hogy a hadseregek az elektronikus harc eszközeihez folyamodnak, évtizedeken át titokban tartották. És hogy az elektronikai lépések védekező vagy támadó jellegűek, mára alig dönthető el.

Az elektronikus harc ott ölt offenzív jelleget, ahol az ellenfél elektromágneses spektrumát a levegőből vagy a földről zavarják, mielőtt támadásra kerülne sor. A líbiai-csádi határháborúban Franciaország háromszor avatkozott be a csádi kormány oldalán, amelyet Moamer Kadhafi – legutóbb 1986-ban – megtámadott. Ennek során az amerikaiak F-111-es harci gépekkel nyújtottak légitámogatást, amelyek a technika akkori állása szerint széles lehetőséggel rendelkeztek zavaró jelek sugárzására – amíg a franciák földi offenzívája ki nem iktatta a teljes elektromágneses spektrumot, s ezzel Líbia összes elektronikus ellenintézkedését, többek közt az ellenséges hadműveletek megfigyelését és azonosítását szolgáló radarállomásokat. Többé senki semmit nem látott – a pillanatot a Francia Idegenlégió egyik veteránja, akit akkor frontkatonaként vetettek be Csád védelmére, „félelmetesen furcsának” nevezte.

Hogy az elektromágneses spektrum zavarait nemcsak nyílt konfliktus esetén idézik elő, hanem azok békeidőben is felléphetnek, jól mutatja egy közjáték, ami 2014 nyarán történt. Érintette a dél-németországi, csehországi és ausztriai légiforgalom volt, a nyári üdülési szezonban, amikor csúcsforgalom van a légtérben.^[46]

2014. június 5-én, csütörtökön váratlanul elnémulnak a polgári légiközlekedés járműveinek rádiójelei. A légiirányítók képernyőiről egyszer csak eltűntek a Bécs, Prága és Pozsony légterében tartózkodó gépek jelei. Ez rendes körülmények közt akkor történik, ha repülőgépek zuhannak le. Ezen a napon azonban továbbra is minden gép a levegőben van. Csak éppen: radar-válaszjeladóik nem sugároznak jeleket és azonosítókódokat. A földi irányítás számára emiatt a gépek láthatatlanok, és valóssá válik az elképzelhető legrosszabb lehetőség, amivel csak egy légiirányító számolhat: az irányítók nem látnak mozgást a légtérben.

Még jó, hogy az utasok az egyre súlyosabb vészhelyzetből semmit sem érzékelnek. Az Austro Control légiirányítóinak vak-sága 25 percig tart: rendszereik kiesése idején olyan analóg eszközökkel kell segíteniük magukon, mint a papír és a ceruza. Ugyanis mialatt a pilóták rádión közlik pozíciójukat és repülési magasságukat, az irányítók manuális listákat vezetnek a fejük felett lévő repülőgépekről.

2014. június 5-én a „légiközlekedés biztonságának” ehhez a „drasztikus korlátozásához” egy magyarországi NATO-gyakorlat vezetett, amelynek során a radar-válaszjeladók elleni elektronikus küzdelmet gyakorolták – állt a történetekről kiadott nyilatkozatban. Amikor azonban néhány nappal később, 2014. június 10-én 13:30 és 15:00 óra közt, ezúttal Bécsben, Prágában és Münchenben ismét eltűntek a repülőgépek a képernyőkről, általános lett a tanácstalanság. Közben ugyanis a NATO-gyakorlat régen befejeződött.

Az összeesküvés-elméletek megfutották szokásos online köreiket. A második zavar a magasan közlekedő légijárműveket érintette. Egy ilyen manőver állítólag csak a világűrből, és műholdak közreműködésével hajtható végre. Márpedig ilyenjei voltak az amerikaiaknak, az oroszoknak és a kínaiaknak is.

A második hibának azonban lehetett természetes magyarázata is. Okozhatták, mint mondták, napviharok, azaz erős, elektromágneses sugárzással járó napkitörések. A Nap 2014-ben csakugyan szokatlanul aktív volt. 2014. június 10-én a NASA három nagy, X-osztályú napvihart észlelt.^[47] Az X-osztályba csak a legerősebb napkitöréseket sorolják. Sugárzási energiájuk ugyan az embernek nem árthat, elég erős azonban ahhoz, hogy befolyásolja a föld elektromágneses mezejét és a földi GPS- és kommunikációs jeleket. Aznap az első napkitörésre az amerikai keleti parti időszámítás szerinti 07:42-kor, azaz közép-európai nyári időszámítás szerint 13:32-kor került sor. Mindössze egy órával később következett egy második, az elsőnél nem sokkal gyengébb robbanás.

Még ha máig sem tisztázott, mi korlátozta a repülésbiztonságot ilyen katasztrofális módon, azért a vele egyidejű heves naptevékenység mégis valószínű ok. Mindenesetre egyaránt hálával tartozunk a légiirányítóknak és a pilótáknak. Még mindig kiválóan ki vannak képezve a mindenféle komputer mellőzésével végzett manuális munkára, sürgőshelyzetben is megbízhatunk bennük.

Elektronikus ellenintézkedések

Az elektronikus harcnak, ami inkább művészet, mint tudomány, az a célja, hogy felfedezzék, lehallgassák, megakadályozzák, esetleg manipulálják az elektromágneses spektrumban folyó kommunikációt, azaz az adatátvitelt. Történhet ez az elektronikus kommunikáció működésének megzavarásával, hamis információk átadásával vagy a kommunikációs hálózat fizikai zavarásával. Különleges szerepet játszik ebben a radartechnológia, ami mesterséges intelligenciával kombinálva kognitív képességekre tesz szert.

Katonai üzemmódban a radarok adaptív sugárzási karakterisztikát mutatnak, ami azonban szigorú titoktartás tárgya. Ez nem újdonság: már évtizedek óta így van. Ha egy radar megváltoztatja üzemmódját, alig észrevehetően változtatja kibocsátott impulzusait, vagy módosítja az úgynevezett *envelope*-ot, a modulációs burkológörbét, amelyen belül rendes körülmények közt működik: ilyenkor egy felderítőrendszer nem egykönnyen deríti fel az ellenséges radart – ha korábban nem „látott” ilyen viselkedést. Ha nem ismerjük egy ilyen radar specifikus sugárzási karakterisztikáját, nemigen lehetséges a zavarása – a *jamming* –, aminek az a célja, hogy az ellenséges érzékelőrendszereket oly módon bombázzuk sugárzással, hogy az ellenfél csak zajokat fogjon, s többé ne tudjon jeleket feldolgozni. Éppen ezért érvényesül olyan szigorú titoktartás a radarrendszerek katonai üzemmódjait illetően. Az információs fölényt az elektronikai

spektrumban nemcsak a magasabb szintű technikának, hanem a titoktartásnak is szavatolnia kell.

Egy radarrendszer, amely csak sémaszerűen variálja karakterisztikáját, nem kognitív. Egy radar csak attól kezdve viselkedik intelligensen, ha alkalmazkodik a helyzetekhez (szituáció-adaptív), mintegy tudatos, akceptálja külvilágát, és működésének módját arra a sugárforrásra állítja be, amelyet figyel. Ha egy kognitív radar megállapítja, hogy – mondjuk – egy felderítő repülőgép közeledik, megváltoztathatja a sugárzási karakterisztikáját, hogy láthatatlanná és azonosíthatatlanná tegye magát.

Támadó fél is folyamodhat elektronikus hadviseléshez, például ellenséges földi radarok felismerése céljából. Egy felderítő repülőgép – ismert típusa a NATO-NE3 AWACS – a légtér egy szektorában haladva sugárzást gyűjt be. A sugárzásban minták rejlenek, amelyeket azonosítani kell. Vajon a Lufthansa egyik légijárata bocsátja ki őket? Vagy egy ellenséges harci géptől származnak? Lehet szó esetleg egy ellenséges földi radarról? Ha a sugárzási minta forrása nem azonosítható pontosan, de egy intelligens felderítőrendszer kialakít bizonyos feltételezéseket a funkciómintázatot illetően, és valószínűsít valamiféle hipotézist azzal kapcsolatban, miről lehet szó, első lépése valószínűleg a sugárzás forrásának provokálása lesz. Ha a sugárzás forrása erre átkapcsol egy másik üzemmódba, a felderítőrendszer végül megállapíthatja, milyen sugárforrással van dolga, és megkezdheti a zavarását.

Hogy a kognitív elektronikus harc egyre nagyobb jelentőséggel bír a killerrobotok elleni küzdelemben, az annak a körül-

ménynek tulajdonítható, hogy a részben autonóm fegyverrendszerek avagy LAWS-ok működésük során éppúgy rá vannak utalva az elektromágneses spektrumra, mint a mi civil környezeti intelligenciánk a maga hálózatba kötött házaival, ipari létesítményeivel és berendezéseivel. Egy távirányítású drón nehéz helyzetbe kerül, ha megszakítják rádiókapcsolatát földi bázisával. Egy hálózatosított autó érdekes dolgokat művelhet, ha zavarják, vagy ha szenzorai hamis információkat fogadnak, mert megtévesztés, *spoofing*-támadás áldozatává lesz.

Sem a környezetiintelligencia-gyártók, sem a kereskedelmi tanácsadó cégek, a digitalizáció élharcosai nem számolnak az elektromágneses spektrum elleni potenciális támadások kockázatával mint magas fokon hálózatosított mindennapjainkat fenyegető kézzelfogható veszéllyel. Németországban csak a Bundeswehr készül fel erre az egyre fontosabb csatatérre, a digitalizáció gazdaságosságot szem előtt tartó civil apostolai viszont nem. Építsünk még több biztonsági elemet a hálózatokba, csak hogy hatástalanítsunk egy kockázatot, amely legfeljebb csekély valószínűséggel jelentkezik? Úgysem történik semmi, minden rendben lesz... hangzik a népszerű vélekedés. Hiszen a digitalizáció infrastruktúráját békeidőben és békeidőre alakították ki. Egyszerűen fogalmazva ez annyit tesz, hogy noha elméletben felismerték a sebezhetőségét, a kockázatmegelőzés egyszerűen nem gazdaságos.

Hálózatbiztonság mesterséges intelligencia révén

A fegyveres erők által alkalmazott mesterséges intelligencia javítja a légtérvédelmet és a katonai technika új és jobb teljesítményeit teszi lehetővé. Kevésbé látványos, de egyre fontosabb, hogy a biztonsági szakemberek is a mesterséges intelligenciára támaszkodjanak a fenyegetéseket automatizált elemzésére. Kártékony szoftvereket kell elhárítani, hogy kivédjék a civil környezeti intelligencia elleni irányuló szabotázszt és kém támadásokat.

Közben ugyanis maguk a támadók is alkalmaznak mesterséges intelligenciát. Átfésülik a közösségi hálózatokat, és civilek személyes adatait gyűjtik össze például *doxing*, magántartalmak nyilvános közlése céljából. Ehhez sok pénzt kell kiadniuk szakemberekre, akik ismerik az adattömeg-analízis, a matematikai modellezés és az algoritmika mesterfogásait. Ezt a kiadást pénzügyileg csak egy állam engedheti meg magának, vagy olyasvalaki, aki egy állam számára kutat és fejleszt.

A környezeti intelligencia nagyobb biztonságához vezető egyik első lépés a saját szoftver minőségének biztosítása. A modern szoftveralkalmazások kódja egyre nagyobb terjedelmű; egy autonóm autó esetében például több millió kódsorból áll. Márpedig minden programozó tudja: hibátlan szoftver nem létezik. Minden szoftver tartalmaz hibát, és soha nincs „kész”. Mármost épp ebben a milliányi potenciálisan hibás és befejezetlen kódsorban kell megkeresni ugyanazokat a hibákat, amelyeket egy támadó arra használhat fel, hogy a kódot megfertőzze

vagy az egész rendszerben kárt tegyen. A minőségbiztosítási feladatok időközben már meghaladják az emberek kapacitását. Komplexebb szoftver kódok tesztelésére, vagy kibocsátásuk előtti minősítésére azonban bevethető a mesterséges intelligencia.

Egy példa: meghatároznak egy bizonyos utasítássort, amelyet egy komplex szoftver kódnak végre kell hajtania, mondjuk 1-től 5-ig. Az instrukciók végrehajtása véletlenszerű, például a 2-5-3-4-1 sorrendben történik. Ha például a 3. utasításnál biztonsági rés jelentkezik, a tesztelőrendszer észleli, hogy melyik parancs a szoftver kód melyik állapotát idézte elő, pontokban kifejezett jutalmat ír jóvá az utasításnak – jelen esetben a 3-asnak –, majd eldönti, hogy következőként melyik utasítást célszerű végrehajtani. Az utasításokat és a nekik megfelelő állapotokat (állapotpárokat), amelyek a komplex szoftver kódban nem mutatnak biztonsági réseket, szankcionálják, mert nem produkálnak sikert, azaz hibaészlelést.

Azoknak az állapotpároknak a kivételével, amelyek már elérték bizonyos pontszámot, a parancsokat különféle sorrendekben, például 1-5-4-2-3 formában, megismétlik. A cél a jutalmazott állapotpárok számának maximalizálása. Ehhez kutatni kell a tesztrendszer lehetőségeit – azaz új kombinációkat kell kipróbálni.

Ez még nem a mesterséges intelligencia, csak az előzetes feldolgozás egy lépése, amelyet Monte Carlo-keresésnek neveznek, a folyamat- és tervezéskutatás egyik technikája. Annyiban jelent kihívást, hogy egy ilyen teszteljárás kezdetén számos véletlen parancskombinációt kell kipróbálni, míg végre felbukkan az

első olyan állapotpár, amely biztonsági rést leplez le. Ezt a keresést le kell rövidíteni és intelligensebbé kell tenni: itt gyorsíthatnak a dolgon a gépi tanulási eljárások. Szakemberek megtaníthatják gépi intelligenciájukat, hogy felismerjék, hogyan festenek egy komplex szoftver kód kritikus állapotai. A mesterséges intelligencia azután célzottan idéz majd elő ilyen állapotokat anélkül, hogy várnia kelljen egy véletlenre, amely hibát fed fel. Ilyen esetekben tehát a mesterséges intelligencia venné át az optimalizációs keresést. Igen, ennyire kevésbé látványos a mesterséges intelligencia, sokkal láthatatlanabb, mint amennyire mi emberek várnánk.

A mesterséges intelligenciának a kódok minőségbiztosításán kívül a jövőben biztonsági szolgáltatásokat is kell nyújtania. Proaktív módon, valós időben kell felismernie és megszakítania a környezeti intelligencia elleni támadásokat. Ez azonban még az élenjáró kutatóintézmények számára is a jövő zenéje, még akkor is, ha egyes IT-biztonsági vállalatok állítják, hogy a mesterséges intelligenciát már használják erre a célra. Nagyzoló állítás ez, hiszen éppen az IT-biztonság az, ahol a mesterséges intelligencia még gyerekcipőben jár. Mindmáig humán specialistákra támaszkodunk: nekik kell felismerniük, elemezniük és szükség esetén viszonzniuk a támadásokat. A 2018-as amerikai választások alkalmával a Facebook egy ilyen, emberekből álló csapatot állított fel. A sokatmondó „Haditanács” nevet viseli.

[NÉGY]

Visszahekkelés

Az ember nem képes kézben tartani egy forradalmat, amíg meg nem érti. (Henry Kissinger)

Nulladik nap. A támadók mélyen befurakodtak az állam hálózataiba. Egyidejűleg több áramszolgáltató is kiesett. Egyes városi hálózatok már egyáltalán nem jutnak áramellátáshoz. Más erőművekre digitális tűz zúdul, s az ellen küzdenek, hogy digitális teljesítményszabályozásukra ismeretlenek tegyék rá a kezüket.

Egyes régiókban órák óta nem működik az internettel való kapcsolatteremtés, s ennek nem pusztán az az oka, hogy a világháló részhálózatainak áramellátása már nem megbízható. A közigazgatás szokatlan módon nem érhető el online – kezdve az önkormányzati igazgatási testületektől egészen az országos hatóságokig. A vonatok állnak, a logisztika csak araszol. A munkahelyi számítógépekről eltűnnek az adatok, már nem, vagy csak váltságdíj ellenében lehet hozzájuk férni. Világszerte esnek a részvényárfolyamok, mert a pénzügyi rendszer tranzakcióinak feldolgozása akadozik. Zavarják az elektromágneses hullámtar-

tományt is, mert a mobil telefonálás sem mindenütt működik. Az okostelefonok haszontalan, felesleges kacatok lettek.

Az infrastruktúra kiesése mindenkit egyaránt érint. Alig akad, aki ne hordaná egész életét a zsebében; olyan az a pillanat, amikor elapad az élet digitális forrása, mint holmi amputáció. Különösen sújtja a helyzet a gazdasági intézményeket: a tévéadóktól a sarki kisboltig. Szakmájuk, iparáguk lebénult. Az emberek pedig el vannak vágva az orvosi ellátástól, az oktatási intézményeiktől és a közlekedési rendszereiktől. A kiesés egész városokat bénít meg, mivel az információáramlás, a folyam, amely a digitális korszakban az életet jelenti, leállt, s vele a digitalizáció révén működő áru- és pénzforgalom is.

Meglepő módon a következményeket a fegyveres erők is megérezték. A légierő számítógépeinek működése ugyanazzal a gyakorisággal szakad meg, mint a civil komputeréké. Egy radarállomások ellen intézett nem kinetikus támadás a repülésbiztonságot is felszámolta. Kockázatos helyzetben van mindenki, aki a levegőben tartózkodik, akár utasként, akár pilótaként. Jobb, ha most a repülőgépek a földön maradnak.

A digitális támadás azonban csak a kezdet. A támadó most már nemcsak arra összpontosít, hogy az áldozatul kiszemelt államban fenntartsa a működési zavarokat, hanem egyszersmind a védelmi képességeit is csökkenteni akarja. Ezért az agresszor támadást intéz az állam elfogó vadászainak digitális szenzorai, jobban mondva azok gyenge pontjai ellen. A hibrid támadás ugyanis csak előkészítette a most következő *double tapet*, a hib-

rid intézkedésekből és a fegyveres erők hagyományos katonai támadásából álló kettős csapást.

Előtte a támadók fedett felderítőakció során meghekkelték az áldozatul kiszemelt állam kormányzati szervereit, és olyan adatokat loptak el róla, amelyek fontosak voltak a hagyományos csapás szempontjából. Most katonák szállják meg a megkárosított ország területét, és gyors ütemben nyomulnak előre a stratégiailag fontos városok felé. A levegőből támogatják őket, ami addig lehetséges, míg a megtámadott állam légtérvédelme meg van gyengülve. Ha szükséges, a támadó rakétaindító támaszpontokat hekkelhet meg, esetleg kihasználhatja a műhold-elhárítási potenciálját. Erős ellenállással nem kell számolnia, mert az érintett lakosság erősen stresszelt, zavarodott és dühös az internet tartós zavara miatt. Már rég megrendült az emberek civil morálja. A médiaszerkesztőségek, ha cselekvőképesek maradtak, szenzációhajhász újságírásra tértek át, és a maguk módján járulnak hozzá, hogy a lakosságon eluralkodjon a pánik.

Az amerikaiak 2012 óta hívják fel a figyelmet egy Cyber Pearl Harbor veszélyére.^[1] Van olyan vélemény, amely szerint 2025-ig számolni kell egy digitalizált infrastruktúrák elleni, sok ember halálával járó támadással.^[2] Az adatok és az új gazdasági csoda reményének mámorában a digitalizáció-ittas társadalom mindeddig elengedte a füle mellett a figyelmeztetéseket.

Ezzel együtt a digitális 9/11-gyel kapcsolatos forgatókönyv nem egy középszerű sci-fi-szerző fantáziájának terméke, aki egy latorállam Amerika vagy Európa elleni támadását demonstrálja. A cselekményvázlat az Egyesült Államok *Nitro Zeus* fedőnevű

haditervéből származik. Ha Irán nem lép a diplomáciai tárgyalások útjára, és nem állítja le atomprogramját, az Egyesült Államok az egész országot le akarja kapcsolni, meg akarja zavarni a védelmi rendszerét, és saját ellenőrzése alá akarja vonni a perzsa államot.^[3] Az amerikaiak, panaszzolják az európai diplomáták, csak ezért gyanúsítanak meg más államokat ugyanolyan támadó tervek birtoklásával, amilyeneket maguk is készek lennének végrehajtani. Mellesleg az irániakkal kötött egyezménynek köszönhető, hogy az Egyesült Államok mindeddig eltekintett egy ellenük végrehajtott átfogó digitális csapástól. Miután azonban Donald Trump felmondta az atomalkut, ismét kézzelfogható közelségbe kerül a hibrid konfliktus forgatókönyve, már csak azért is, mert az elnök demonstrálni akarja országa erejét, és agresszívebben lép fel, mint hivatali elődei.

De azért nem valószínű, hogy ugyanúgy fog megtörténni, ahogyan bemutattuk. Egy országot egyik pillanatról a másikra aligha vetnek vissza analóg állapotba. Realisztikusabb, hogy a káosz kevésbé feltűnően bontakozik ki. Nem működnek majd zökkenőmentesen a számítógépek, a termelési folyamatok és a logisztika; a weboldalak túlterheltek lesznek, és nem lehet megnyitni őket, vagy idegen propaganda jelenik meg rajtuk. Az országban nehezebbé válik a munka, lelassulnak a mindennapok. Egy hekkerakció vagy digitális zsarolás ma már ritkán irányul konkrét stratégiai célok ellen, ahogyan a Stuxnet és az iráni urándúsító létesítmények esetében történt. A vírusok, férgek és zsarolószoftverek a véletlen törvényét követik, és válogatás nélkül megfertőznek minden gépet, amibe be tudnak férkőzni. Ez-

után már senki sem tudja megjósolni, hogyan bontakozik ki egy ilyen támadás – még maga a támadó sem. És megfordítva – a megtámadott ország sem fogja fel azonnal, hogy hibrid támadás áldozatává vált.

Mindkét támadási forgatókönyv egyformán stresszt, haragot és félelmet vált ki a lakosságból. A normalitás minimumának visszaállítása érdekében a szorongatott helyzetben lévők azzal kezdik majd, hogy az infrastruktúra kieséseit, különösen a „fekete startot” – azaz az energiaellátás napokig, hetekig tartó szünetelését – áthidalják. Az internet és az e-mail kiesését műholdas kommunikáció kompenzálhatja. Külföldi szimpatizánsok nyújthatnak digitális támogatást, s e tekintetben valószínűleg nemcsak szövetséges államokról, hanem nem állami szereplőkről is szó lehet. Az infrastruktúra-működtetők, a gazdasági szféra, a hatóságok és a baráti államok a közössége, amelyet békeidőben működtettek, kooperációjukat pedig szimulációs gyakorlatok során tesztelték, erőfeszítéseket tesz, miközben a megtámadott nemzet keresi a választ a kérdésre: ki a felelős? Mi legyen a megtorlás? Hogyan lehet felkészülni a válaszcsapásra?

Joghézagok: a nemzetközi jog tökéletlensége

„Belbiztonsági hírszerző szolgálatként mi nem vagyunk egy offenzív hatóság. Nincs jogosítványunk úgynevezett visszahekkelésre, *hack backre*, tehát arra, hogy offenzívát indítsunk valamely szembenálló hírszerző szolgálat információs technológiája

ellen, és elpusztítsuk”, mondja Hans-Georg Maaßen, a Szövetségi Alkotmányvédelmi hivatal egykori elnöke, és hozzáteszi: „A Bundeswehr, amely rendelkezik a know-how-val, és van elég anyagi forrása, nem törődhet hibrid támadásokkal, mert nem indukálnak védelmi helyzetet. Jóllehet a Szövetségi Alkotmányvédelmi Hivatal mint polgári elhárító szolgálat illetékes az ilyen esetekben, de nem rendelkezik a Bundeswehrével összevethető forrásokkal. Ezért szoros együttműködést tartunk fenn a Bundeswehrrel.”^[4]

Nem jogilag szabályozatlan közegben kerül sor hibrid intézkedésekre, és az elhárításukra sem, ezzel együtt nyitott kérdések sokaságát vetik fel.

„A *Cyber* kimutatta, hogy a jogi szabályozás nem egészen egyértelmű”, állapítja meg ezzel kapcsolatban Tobias Vestner svájci nemzetközi jogász.^[5] Ugyanis: már egy államilag szponzorált hekkertámadás jogi besorolása esetén is jogizonytalanság jelentkezik. Vajon háborús cselekmény egy hekk? „Például: 2008-ban Oroszország ezt követett-e el Grúzia ellen? Azt hiszem, a legtöbben igennel felelnének. Elég ez rakéták kilövéséhez, és az átváltáshoz a cybertérrel a valóságos, fizikai térre?”^[6]

„Valóban háború ez?”, teszi fel a kérdést Heiko Borchert védelmi tanácsadó is. „Ez attól függ, miképpen tudok védekezni, vagy miféle megtorlást tudok alkalmazni. Az értelmezési szuverenitásért folytatott versengést a jövő egyik legfontosabb, ha ugyan nem a központi csataterének tartom. (...) Vagy az egyik, vagy a másik irányba interpretálok. Ha háborús, akkor az ügynek a fegyveres erőkhöz is van kapcsolódási pontja.”^[7]

A korábbi német szövetségi elnöknek ezzel kapcsolatban van precíz válasza. „»Nem hibrid háborúról« beszélünk, mert nem vagyunk hadiállapotban. A hadiállapotot mindenképpen – legalábbis kifelé – el kell kerülnünk. Ehelyett hibrid fenyegetésnek nevezzük, amikor a háborús küszöböt nem éri el, de túlmegegy azon, amit megengedhető befolyásolásnak, illetve megengedhető aktív intézkedésnek tekintünk.”^[8]

Tehát szürkezónában mozgunk. Jó oka van, hogy az olyan jogászok, mint Hans-Georg Maaßen, elővigyázatosan bánnak a háború fogalmával. Egy katonai támadás ugyanis komoly következményekkel járna, igazolná például az önvédelem jogosultságát. Egy állam ellen hibrid eszközökkel indított pusztító támadás esetén az önvédelem a visszahekkelésztől, a *hacking back*től, a konvencionális második csapásig terjedhetne. Ugyanazt ugyanis nem kell ugyanazzal megtorolni, és a hibrid támadásra adott válasznak nem kell szükségképpen hibridnek lennie. Tekintetbe kell azonban venni az arányos, azonnali és megfelelő védelem elvét.

Senki sem szívesen gondol bele alaposabban, hogy egy hibrid támadás forró háborúba torkollhat. A kényes témát nem szívesen taglalják. Tobias Vestner ezt így foglalja össze: „Ameddig nincsenek fizikai károk, még mindig mondhatjuk: ez nem fegyveres konfliktus, ez nem háború.”^[9] Csakhogy ilyenkor éppen az illetékesség kérdései maradnak megválaszolatlanul: tulajdonképpen ki hárítja el a hibrid támadásokat?

Hogy miképpen kezeli a kérdést a német politika? Az Alkotmányvédelmi Hivatal volt elnöke korábbi elnöke szerint: „Hib-

rid fenyegetés esetén – és hangsúlyoznom kell, hogy itt (...), nem, nem akarom azt mondani, hogy új területre lépünk, de a szövetségi kormány, a törvényhozó még nem indult el ezeken az ösvényeken, és pláne nem taposta ki őket – az illetékességek abszolút megosztása értelmében a belföldi hírszerző szolgálat, tehát a Szövetségi Alkotmányvédelmi Hivatal az illetékes elhárító hatóság.”^[10]

Egy külföldi kormány háborúszerű lépéseket tesz, finoman és a háborús küszöb alatt, az ellenintézkedések azonban egy civil hatóság, nem pedig a fegyveres erők hatáskörébe tartoznak.^[11] A támadás jellege és a védekezési lehetőségek közti diszkrepancia az alkotmányvédelmi hivatal bármelyik elnökét igen csak nyugtalaníthatná.

S vajon mi a helyzet azokkal az információs térben végrehajtott műveletekkel, amelyek egy országban a demokratikus választásokat zavarják? Ilyenkor vajon egy állam belügyeibe való meg nem engedett beavatkozásról van szó? Milyen állami intézmények felelősek a veszély elhárításáért, a második csapásért, a megelőző csapásért vagy a hibrid támadások megelőzését célzó elrettentésért? Végül pedig: ki ellen irányuljon a megtorlás?

„Ha egy állam nem biztos abban, ki támadta meg, vét a nemzetközi jog ellen, ha egy támadás elhárítása céljából csapást mér valakire, akinek esetleg még csak köze sem volt a támadáshoz.” Wolfgang Ischinger joggal aggasztja, hogy nehéz megállapítani, kinek tulajdoníthatók a hibrid támadások, amelyek a hekkertámadásoktól a külföldön élő rendszerellenes elemek célzott megölésén át a felségjelzés nélküli fegyveres haderő bevetéséig min-

denféle eszközt magukban foglalhatnak. Annak a feje felett, aki második csapást hajt végre anélkül, hogy hitelt érdemlően bizonyítani tudná, kitől indult ki az első, Damoklész kardjaként függ, hogy esetleg háborús bűnt követ el.

Emellett az, ha az agresszorok tagadják a hibrid támadásokat, külön kárt okoz az áldozatnak, amely így az önvédelem érvével csak nehezen győzheti meg a nemzetközi közösséget. „Tagadj, tagadj és tagadj (...). Ha valamit beismersz vagy bűnösnek vallod magad, halott vagy. (...) Tagadj mindent, amit csak mondanak rólad. Soha semmit ne ismerj el.” Ne feledjük, hogy Donald Trump ezt a tanácsot adta egy barátjának. Ha a politikában fogadják meg, drasztikus következményekkel jár. A tagadás nyomán bizonytalanság támad. Valamennyi kétely mindig megmarad. A következmény: egy agresszív állam anélkül képes elérni területvédelmi és befolyásszerzési céljait, hogy akárcsak egyetlen tartalékost is mozgósítana. És meg is van minden esélye, hogy megússza büntetlenül.

Ennek ellenére könnyen vesszük a szánkra a „cyberháború” szót, és így tesz a hagyományos média is: „Háborúról beszélni kétségkívül helyes.”^[12] Valóban így van? Manapság valóban folyamatosan alacsony intenzitású kvázi-háborús cselekményeknek vagyunk kitéve, és rég hozzászoktunk, hogy már a holnapi nap biztonságos átvészelését is egyre fontosabbnak tartjuk? Nincsen többé egyértelmű határ a háború és a béke közt, és dichotómia helyett egy háború–béke-kontinuumban élünk, a napi szurkálások pedig, amelyeket elviselünk, tartós állapotá válnak? Vagy a háborúról folyó beszéd csak metafora, mint a „há-

ború a Német Labdarúgó Szövetség ellen”, vagy a „háború a drogok ellen”?

Az agresszív államközi intézkedéseket szabályozza a nemzetközi jog, ennek alkalmazási és érvényesítési esélyei azonban csekélyeknek tűnnek. Herfried Müller német politológus ezért a hadurak vagy terroristák új háborúit illetően azzal érvel, hogy a nemzetközi jog kiüresedett, az állam elveszítette erőszakmonopóliumát, a „front”, a „hadviselő”, az „egy hadszíntérre való összpontosítás” fogalmai tartalmukat veszítették, és manapság sem a nemzetközi hadijogot, sem a nemzetközi humanitárius jogot nem tartják tiszteletben.^[13]

Egy véleményen van vele jó néhány amerikai nemzetközi jogász is. A nemzetközi humanitárius jog az újfajta háborúkra, nevezetesen a terror elleni háborúra nem alkalmazható, mert az ellenfél, nem nemzetállam, hanem nem állami szereplő. A jognak ezzel a szó szerinti értelmezésével az amerikaiak saját szárazföldi csapatainak bűncselekményeit akarják kimagyarázni, akik az iraki Abu Ghraib fogolytábor rabjait alantas indokokból kínozták.^[14]

Az emberi jogokat valóban számtalan esetben megsértik – a humanitárius nemzetközi jog éppen ezt kívánja megakadályozni. Az ilyen jogsértések köre már a 21. században is az amerikai titkosszolgálatok által végrehajtott emberrablásoktól amerikai börtönök harmadik országokban való működtetésén és olyan őrizeteselek fogva tartásán át – akik számára sohasem biztosították a tisztességes eljárást – egészen a kínzásokig terjed. Ha pedig csakugyan végrehajtják Donald Trump utasítását, lőfegyve-

reket használnak majd azok ellen a menekültek ellen, akik a mexikói–amerikai határon kövekkel dobálják a határőröket. A szíriai Aszad-rezsim mérgesgáz-támadásai éppúgy szerepelnek a felháborító emberijog-sértések listáján, mint a háborús menekültek visszatoloncolása a Líbiához hasonló működésképtelen né vált államokba.

Anélkül azonban, hogy bagatellizálnánk azokat az incidenseket, amelyek során emberi jogokat sértettek meg, mégis csak feltűnő, hogy mindig éppen az az Egyesült Államok keveredik újra meg újra különösen szörnyű emberijog-sértési ügyekbe, amely az emberi jogokat nyilvánította társadalmának alapkövévé.^[15] Hogy ezt megértsük, érdemes röviden egy pillantást vetnünk a háború kultúrája és a technológia fejlődésének összefüggésére.

Annak értelmezése, hogy miért és hogyan viselnek háborúkat, egy-egy nép kultúráját alapul véve elég különböző volt a történelem során. Az aztékoknál a háborúnak rituális jellege volt. A kínai Han-dinasztia idején úgy gondolták, a hadviselés az égi rend fenntartását jelenti.^[16] Európában a terjeszkedés és a területvédelem volt a lényeg. Ezzel szemben az Egyesült Államok számára mindig központi jelentőséggel bírt a liberális értékek megőrzése. Az európaiakkal ellentétben az amerikaiak számára a háború egyáltalán nem a politika más eszközökkel való folytatását jelentette, hanem sokkal inkább felmentést a politika alól. Az ő szemükben a háború mocskos ügy volt, ami nem felel meg egy köztársaság elvárásainak. A lehető leggyorsabban be kell fejezni. Imperatívusza: a döntő győzelem,^[17] a feltétel nél-

küli kapituláció. Vagy, ahogy Hannah Arendt fogalmaz: „A győzelemnek nincsen alternatívája.”^[18]

S vajon mi szolgált a legfényesebb kilátásokkal arra nézve, hogy sikerrel vívhatnak kontrollált háborúkat, s arathatnak gyors győzelmeket? A választ e kérdésre Amerika a maga technológiai fölényében kereste. Nagy kiterjedésű, gyéren lakott ország lévén, ha gazdasági növekedésre törekedett, mindenképpen rá volt utalva a gépesítésre, az automatizálásra és a szabványosított gyártási folyamatokra, s ezért ezeket ambiciózus módon előmozdította. A kifinomult technika következtében azonban az amerikai hadviselés rendkívül pusztítóvá vált; az Egyesült Államok volt az egyetlen nemzet, amely valaha is atombombát dobott le ellenséges területre.

A szabadelvű-demokrata beállítottságú Amerika számára máig dilemmát jelent, hogy háborúit, mielőbbi befejezésük érdekében, nagy erőkkkel vívja, egyidejűleg azonban kénytelen tiszteletben tartani a humanitárius nemzetközi jogot, amely pontosan azokat az értékeket oltalmazza, amelyek védhatalmakként az Egyesült Államok mindig is fellépett. Az emberi jogok voltak, amelyek Amerika számára évtizedeken át egy globális rendfenntartó hatalom *soft power*jét biztosították. Ebből is dilemma származott, mert a nemzetközi jog absztrakt módon és előrelátóan rendelkezik arról, hogy egyáltalán mely fegyverzeti technológiák juthatnak el a bevetésig. Az elsőprő győzelem rendjén való – nem így azonban a fegyverek, amelyek ellenkezőnek a liberális-felvilágosult értékekkel. Végére is az emberi jo-

gok fontosságára való tekintettel mégsem szabad mindent megengedni.^[19]

Következésképpen a nemzetközi jogi korlátozás összeütközésbe kerül az amerikaiak „még jobb háború” és egyre vezetőbb fegyverek iránti igényével, amelyek közé a LAWS-ok is számítanak. Ez végső soron azt is megmagyarázza, miért nem akar részt venni az Egyesült Államok a LAWS-ok betiltásában: úgy tűnik, a digitális villámháború kézzelfogható közelségbe került. Ezért annak megtagadását, hogy tilalom aláíró országaként lépjen fel, egyszerűen az amerikai hadviselési kultúrának róhatjuk fel.

Közben az egész földgolyó magáévá tette a hadviselésnek azokat a normáit, amelyeket Amerika szabott meg, és lecsiszolta a korábbi kulturális különbségeket. Csekélyebb technológiai jártassággal rendelkező ellenfelek elsajátították az amerikai hadviselési kultúrát, és aszimmetrikus eszközökkel célozzák meg a magas szinten automatizált, hatékony hadviselés technikai utópiáját. Így tekintve a hibriditás közvetlen következménye az Egyesült Államok, „a tudomány köztársasága” technológiai erejének – egyúttal azonban a legsúlyosabb gyengéjévé is vált. Egy konfliktus esetén ugyanis a digitalizáció jóval kevésbé eszköz, mint inkább Achilles-sarok lehet: az ország régóta előreviszi és exportálja a minden internetjéhez való csatlakozást, mára viszont ez a hálózatiság jelentős probléma lett.

Ugyanez érvényes a hagyományos Nyugatra is. Gazdagsága immár nem jelent előnyt számára. Bizonyos, hogy a szegényebb országok kevesebb technológiát engedhetnek meg maguknak,

ugyanezen okból azonban kevésbé sebezhetők. Semmi sem szab azonban határt a kreativitásuknak, amivel kihasználják a technológiailag fejlettebb országok gyengéit, és súlyos károkat okoznak nekik.

Térjünk vissza a nemzetközi jog hibrid fegyverekre alkalmazhatóságának kérdéséhez. A jognak az a feladata, hogy „ismerje és leképezze a valóságot”^[20]. A hibriditás azonban szűrkezőna. Amennyiben „a hibriditás (...) annak a dolognak a definiálhatatlanságára utal, amelyet leír”, és inkább olyasvalamire vonatkozik, ami már nem létezik – ahelyett, hogy precízen leírná, ami az új a megváltozott szituációban”,^[21] a jogi rendszert kérdőjelezi meg. Röviden, ilyen értelemben a hibriditásnak nincsen megfelelője a nemzetközi jogban.

Az emberi jogi ügyvédek és nemzetközi jogászok elszántan tiltakoznak ez ellen. A szűrkezőnával kapcsolatos jogpozitvista érv, amiből szerintük a nemzetközi jog elégtelensége és így alkalmazhatatlansága következik, nem máshoz vezet, mint jogi nihilizmushoz, és a nemzetközi jognak az újonnan létrehozott tények előtti kapitulációjához.

„A jognak mindig két lábbal a földön kell állnia, és nem szabad elveszítenie kapcsolatát a valósággal”, veti ellen Tobias Vestner nemzetközi jogász is, aki ez okból kodifikált normáinak szó szerinti megfogalmazásán túllépve értelmezi a nemzetközi jogot. „Ha egy cybertámadás vagy egy mesterséges intelligencia által végrehajtott támadás nyomán ténylegesen fizikai károk keletkeznek, akkor elérkeztünk a tárgyi szférába, és harckocsikkal is visszavághatunk.”^[22]

Ilyen megközelítésben az államok által indított hibrid támadások inkább a nemzetközi jog reneszánszát, semmint érvénytelenné válását idézik elő, hiszen az pontosan azt akarja szabályozni, ami a hibrid valóságnak megfelel: az államközi konfliktusokat. A konfliktus jellegén – legyen bár hibrid vagy hagyományos, nyíltan, vagy államilag szponzorált csoportok által fedetten végrehajtott – ez nem múlhat. Mindenesetre továbbra is kérdés, hogy jogilag miként sorolható be. A nemzetközi jog egyszerűen nem kapitulálhat a viszonyok változása előtt, inkább olyan eszközöket és hatásköröket kell keresnie a béketeremtéshez, amelyek az haladás okozta változás korszakában is tartósan beválnak.

A nemzetközi jog szakértőinek pedig bizonyos mértékig kötelességük, hogy nyomatékosan ragaszkodjanak a nemzetközi jog érvényesüléséhez. A jognak ugyanis pontosan akkor kell érvényesülnie, amikor a politika azzal ellentétes célokat követ. Nem a választások tesznek ugyanis bennünket szabadelvű demokráciákká, még csak nem is a többség uralma – ha az zsarnoki. A jog érvényesülése teszi, a hatalom megosztása, szabadságjogaink garanciái és a polgároknak az a joga, hogy közreműködjenek a hatalom gyakorlásában. A jog a köz harmadik oszlopként erősíti demokratikus államrendünket. Ha nem sikerül érvényt szerezni neki, közösségünk összeomlik. Ha megszegjük a nemzetközi jogot, a béke omlik össze.

A nemzetközi jog ellentéteket szüntet meg, hogy a békét, mint jog által védett becses érdeket, fenntartsa. Az erőszak csak az önvédelem kivételes esetében indokolt, máskülönben a béke

megsértése hatályba helyezi az ENSZ Biztonsági Tanácsának erőszak-monopóliumát, aminek szankciók és ENSZ-határozatok a diplomáciai következményei. A nemzetközi jog nem engedhet és nem is szabad, hogy engedjen nemzeti érdekeknek, ellenkező esetben ugyanis önmagát adná fel. Egy olyan kormány, amely csak saját nemzeti érdekeit követi, s ennek érdekében rendszeresen a reakcióküszöb alatt tevékenykedik, kihasználja a szabályozás réseit vagy egy norma bizonytalan jelentését, és megbízott vagy delegált zsoldosaira mutogatva minden felelősséget elhárít magától, visszaél a joggal. A nemzetek ezt nem vehetik tudomásul. „A jognak éppen ilyenkor kell jognak bizonyulnia, olyan hatalomnak, amely a politika felett áll, ellenőrzi és a méltányosság szabta korlátok közé szorítja”, erősíti meg a jogtudós Friedrich von Westphalen gróf.^[23]

Másfelől az is igaz, hogy a nemzetközi közösség még nem dolgozta ki az egyértelmű elméleti alapot, amely világos reakciót tesz lehetővé az új fenyegetésekre. „A NATO hihetetlen cyberpotenciállal rendelkezik, hihetetlen cyberstratégiával azonban nem”, állapította meg Philip Breedlove, a NATO volt parancsnoka 2017 májusában. „Stratégiánk valóban meglehetősen körülhatárolt. Szövetségként nem igazán mérlegelhetünk offenzív lépéseket a cybertartományban.”^[24]

Nem vezet sehová, ha hallgatunk a kényes témáról. A nemzetek ezért beszélnek arról, hogyan változtatja meg az új, digitális valóság a hadviselést is, és hogy miként kell erre reagálnia a jognak – akkor is, ha ma még senki nem tudja pontosan, mit jelent konkrétan a hibriditás. Mindenesetre a NATO már 2014-es

walesi csúcstalálkozóján megpróbálta szavakba foglalni a nehezen meghatározhatót: „A hibrid hadviselés jelentette fenyegetés nyílt és fedett, katonai, paramilitáris és civil intézkedések sokasága, magas szinten integrált formába rendezve.”^[25] Minden olyan eszköz egy állam kezében, amely nemzeti célok megvalósítását szolgálja – anélkül azonban, hogy forró háborút robbantának ki vele –, a hibrid szerszámoszláda tartozéka.

Vajon a hibrid támadások jelentik a kiindulópontot ahhoz, hogy megértsük, mi történik velünk? És ennyi már elég-e ahhoz, hogy megtalálhassuk át- meg átdigitalizált társadalmunk gyenge pontjait?

Ahhoz, hogy normákat állíthassunk fel, először tisztán kell látnunk.

Ius ad bellum: az erőszak tilalma

A hatalom abszolút, abban az értelemben, hogy egész, teljes és tovább nem fokozható. Viszont nem feltétel nélküli. Demokratikus társadalmakban keletkezésének szükségszerűen kell, hogy legyen egy konkrét pillanata. Személyek találkozásának pillanatában jön létre. A hatalom egy csoport összegyűlésével kezdődik. Eleve csak ott, a közösségben válik lehetővé egy személy nyilvános cselekvése „a világban” – aminthogy interszubjektív szabadságának a gyakorlása is, hogy gyülekezzen, eszmét cseréljen, véleményt nyilvánítson.^[26]

Ezen a digitális korszak sem változtat. Hatalmas erővel lép fel a Snowflake-generáció több tízezer diákja a klímademonstrációkon; mindegyikük olyan páratlannak, olyannyira egyedülállónak tekinti magát, amilyen egy hópehely. A March for Life, az Élet Menete alkalmával amerikaiak százezrei tüntetnek szigorúbb fegyvertörvényekért. A YouTube-ra tartalmakat töltők demonstrációt szerveznek a szerzői jog uniós reformja ellen. Nem elég persze az interneten hatalmasnak lenni, ezer követő és barát csak egy absztrakt szám, s akit csak véleménybuborékokban és visszhangkamrákban, algoritmikusan menedzselnek, láthatatlan marad a világ számára.

Miközben a demokráciában a hatalom kölcsönös meggyőzésre és befolyásolásra épít, és véleményekről tárgyal, amelyeknek képviselői közül a sikeres szereplők „rávesznek másokat, hogy úgy cselekedjenek, ahogyan akarom”^[27], az erőszak, ami a hatalom antitézise, mindig jelen van. A hatalomnak és az erőszaknak ugyanaz a célja: mindkettő befolyásolni akar másokat. A hatalmasok meggyőznek, az erőszakosok arra törekszenek, hogy rákényszerítsék akaratukat az ellenfélre. És épp a kényszerítés adja a háború lényegét. Az erőszak megzavarja a rábeszélés és meggyőzés folyamatát. Helyébe tárgyak, az invázió, a megszállás, a rombolás és a gyilkolás katonai eszközei lépnek. De vajon ide tartoznak-e az olyan eszközök is, mint a számítógépes program, a robotok, a mesterséges intelligencia?

»*War is killing*«, a háború gyilkolás, fogalmaz zavarba ejtő élességgel Martin van Creveld hadtörténész.^[28] Ha ez így van,

akkor az új digitális eszközök talán már az erőszak-fogalommal sem egyeztethetők össze.

Látván, hogy a háború még a 20. század első felében is a külpolitikai érdekek érvényesítésének bevált eszközének számított, a nemzetek 1945-ben úgy döntöttek, hogy a világ nem ragadhat le a háborúknál. Az Egyesült Nemzetek Chartájával korszakalkotó nemzetközi alapnormát léptettek hatályba, nevezetesen az erőszak kötelező tilalmát, mégpedig azzal a céllal, hogy a népek külpolitikai cselekvésének vezérelve legyen. „Nemzetközi kapcsolataiban valamennyi tag lemond a másik állam területi sértetlensége vagy politikai függetlensége ellen irányuló, vagy az Egyesült Nemzetek céljaival egyéb okból összeegyeztethetetlen erőszakkal való fenyegetésről és az erőszak alkalmazásáról.”^[29]

A nagyobb katonai cselekvési mozgástér biztosítása érdekében az utóbbi időben elsősorban amerikai nemzetközi jogászok helyezkednek arra az álláspontra, hogy az erőszak tilalma erejét veszítette.^[30] Immár kivihetetlen, állapítják meg a pragmatikusok lényegre törően. Pesszimizmusuk abból ered, hogy a nemzetközi jogi erőszakfogalom jelentéstartalma túl szűkre szabott.

Egy ilyen álláspont azonban semmiképpen sem jelenti, hogy az erőszak fogalma mindenféle értelmezés, analógia vagy további kimunkálás alól kivonja magát: „fellebbez” a jogalkalmazókhoz, hogy az erőszak tilalmának általános elveit a 21. századra is átszármaztassák. Jogi fogalomként ugyanis az erőszak tilalma igényli – és alkalmas is rá –, hogy értelmezzék. Ez a tulajdonsága egyébként megkülönbözteti a klasszikus, írott jogot a programkódtól. A programnyelven, azaz a forráskód partitúrá-

ján nincs mit magyarázni – a legtöbb esetben legalábbis nincsen. (A mesterséges intelligencia esetében ez lehet másképpen.)

A jogi nihilistákon kívül létezik egy másik frakció is, amelyik szorgalmazza a 21. század új, nemzetközi jogilag kötelező normáinak megteremtését. Mindazonáltal a nullával egyenlő annak valószínűsége, hogy a kezdeményezést siker koszorúzhatja. Az *America First! Italy First! Hungary First!* globális rendszerében a nemzeti egoizmusok nagyobb súllyal esnek latba a közös dolgoknál. A nemzetközi konszenzusképtelenséget nem egyedül az bizonyítja, hogy mindmáig nem sikerült törvényen kívül helyezni a LAWS-okat. A *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Tallinni kézikönyv 2.0 a nemzetközi jog alkalmazásáról a cyber-hadműveletekre), amely a digitális támadásokat, mint a hibrid eljárások arzenáljából származó eszközöket sorolja be, nem több, mint szakértők semmire sem kötelező kommentárműve. Kézikönyv – aligha van, ami ennél kevésbé kényszerítő erejű. Tekintettel az érdekek ilyen súlyos konfliktusára, a jogi racionalitás egyetlen lehetőséget kínálhat: jobb a létezőt bővíteni, mint új törvény megalkotásával kísérletezve kudarcot vallani.

A robbanás erejével

„A masszív katonai erőszak” az, amit a nemzetközi jog tilt, és egyebütt „fegyveres támadásnak”^[31] nevez. A NATO-szerződés

5. cikkelyében a NATO-partnerek megismétlik, „hogyan egy fegyveres támadás közülük egy vagy több európai vagy észak-amerikai ország ellen valamennyiük elleni támadásnak tekintenek”. A fegyveres támadás fogalmát hagyományosan így értelmezik: a fegyveres támadás mozgási energiát szabadít fel és fizikai hatást gyakorol az érintettre, pontosabban: az érintett objektumra.

Konkrétan: bombáznak vagy ágyúznak egy ipari létesítményt, amely elpusztul. Egy Hellfire-rakéta célba vesz egy hadviselő személyt, eltalálja, és végez vele. Egy fegyveres támadás elpusztítja célobjektumait, esetleg emberek halnak és sebesülnek meg. Gyorsan világossá válik, hogy ez az értelmezés nem alkalmazható közvetlenül a hibrid támadásokra. Adatlopás, zsarolószoftver vagy Facebook-propaganda még soha nem okozott emberhalált. Ameddig egy támadás zajlik vagy közvetlenül küszöbön áll,^[32] a neki kitett államnak szabad önvédelmi intézkedésekhez folyamodnia. Joga van hozzá. Ennek során döntő fontosságú az időablak: meghatározza, mi számít indokolt önvédelemnek, és mi tiltott bosszúnak. A megtorlásnak ugyanis nem létezik törvényes alapja. Egy ellenséges támadás ellen, amely már nincsen folyamatban, már nem védekezhetünk, ilyenkor már csak megfizetni akarunk a másoknak. A nemzetközi közösség ezt nem fogja tűrni.

Önvédelem céljából az erőszak mindenesetre csak akkor válik szükségessé, ha támadás még nem következett be, de közvetlenül küszöbön áll, és a feltételezhető áldozat nem lát más kiutat, mint az erőszakot. Ha a feltételezhető áldozat egy hír-

szerző szolgálata olyan értesülésekre tesz szert, hogy néhány napon belül szabotázs-támadás éri az ország földgáz-vezetékét, megelőzésképpen folyamodhat az állam, mint leendő áldozat, erőszakhoz, és például semlegesítheti a személyeket, akik a támadást végrehajtani készülnek.^[33] Az tehát már megengedett – hogy a támadásokat megállítsák, még mielőtt elérik céljukat.

Emellett a megelőző önvédelem mellett, amelyre az ENSZ Alapokmányának 51. cikkelye vonatkozik, ugyancsak érvényben van az Egyesült Államoknak az „aktív megelőző védekezés” (*defend forward* vagy *active defense*) doktrínája is. A külföldről indított hibrid támadások ellen – és ezek közé tartoznak például a választási infrastruktúra elleni támadások – az Egyesült Államok ellentámadást szándékszik indítani. Ebben az értelemben a *hacking back* az aktív védelem eszközei közé tartozna.^[34] Ennek során mindazonáltal a technikai kivitel jelenti a kisebb kihívást. Sokkal fontosabb kérdés, hogy milyen politikai következményekkel jár egy megelőző védelmi intézkedés, hogyan reagál az ellenséges állam, s hogy vajon az eskaláció minden formájára készen áll-e maga a preventív szereplő.

Mármost: mi a helyzet a hibrid lépésekkel? Vajon a digitális kémkedés, szabotázs vagy felforgatás eleget tesz-e a fegyveres támadás feltételeinek? Vajon egy hibrid akció mikor tiltott erőszakcselekmény, ami hatályba lépteti az áldozatállam jogát a védekezésre? Avagy a hibrid lépések jogszerűek?

Aki be akarja tiltani a fegyveres támadásokat, ezzel egyszersmind azt is mondja, hogy vannak az erőszaknak olyan formái, amelyek mások, mint egy fegyveres támadás. Ekkor kötelezően

felvetődik a kérdés, hogy mikor kategorizálható egy hibrid attack fegyveres támadásként.

Az Egyesült Nemzetek erőszaktilalmának taktikájához tartozik, hogy az államok egy fegyveres támadásnak nem a hatását ítélik meg: annak eldöntése ugyanis, hogy az agresszor milyen intenzitású kényszert fejt ki, illetve milyen mértékben akadályoz, dönt romba vagy pusztít el egy másik országot, végső soron az áldozatállam meglehetősen szubjektív megítélésének tárgya, és a többi nemzet számára nehezen lenne ellenőrizhető. Ráadásul időbe telhet, mire egy fegyveres támadás hatása teljes mértékben kibontakozik. Ezért más mércét alkalmaznak, s azt nézik, milyen eszközzel követték el az erőszakot. Ennek megállapítása, úgy tűnik, könnyű, gyors és objektív.

Egyetértés uralkodik azzal kapcsolatban, hogy vannak eszközök, amelyeknek a használata nem számít erőszak-alkalmazásnak. Ide tartozik egy állam minden gazdasági vagy politikai intézkedése. Időközben a hibrid eszköztárból is társultak bizonyos instrumentumok a nem erőszakos befolyásgyakorlás megengedett eszközeihez. A tudósok a „legitimitás vélelméről” beszélnek, ami a hírszerzési folyamatokra, a kémkedésre, az adatlopásra, a lélektani hadműveletekre és a propagandára terjed ki.^[35]

Általában véve is kihat ez a hibrid eljárások megítélésére: Hillary Clinton e-mailjeinek ellopása nem volt erőszakcselekmény. Bizalmas tartalmuk nyilvánosságra hozatala és közszemlére tétele éppoly kevésbé volt erőszak, mint az, amikor az orosz katonai titkosszolgálat a 2016-os amerikai elnökválasztási kam-

pány idején hamis identitások alkalmazásával hirdetéseket jelentetett meg a Facebookon. A kártékony szoftveres orosz behatolás a amerikai DNC számítógépeibe nem volt egyenértékű egy fegyveres támadással. Még az irániaknak a New York-i tőzsde és több Wall Street-i bank ellen intézett, 2001-es túlterheléses támadása^[36] sem jelentette erőszak alkalmazását, jóllehet súlyos károk érték az Egyesül Államok nemzetgazdaságát miatta. Aki csak gazdasági károkat okoz, nem vét az erőszak tilalma ellen. Ugyanez érvényes a WannaCry-ra, Észak-Korea zsarolószoftvére.

Időközben elfogadottá vált, hogy a fizikai erőszaknak vannak nem fegyveres, nem katonai, a fegyveres támadások szintje alatti formái: amikor például ellenőrizetlenül megnyitnak egy gátat, és árvíz keletkezik. Vagy megszakítják az áramellátást, ezért szünetelnek a kórházakban azt életbevágóan fontos operációk. Megzavarják a légiirányítást, és lezuhan egy személyszállító gép.

Hogy most ismét foglalkozzunk a háború és béke dualizmusával – amelyet még ma is számos állam vall –, a hibriditás szűrkezőnája a két állapot között húzódik. Az egyik a béke a politika és a gazdaság megengedett eszközeivel, valamint a legitimitás vélelme alá eső instrumentumaival, a „megengedhető, normális befolyásolási intézkedésekkel”, ahogyan Hans-Georg Maaßen helyesen megnevezi őket – a másik a háború a maga hagyományos, fizikai erőszakgyakorlásra alkalmas szerszámaival.

Közben globálisan kialakulóban van az a jogfelfogás, amely szerint a szabotázs olyan esetei, amelyeket a Stuxnethez hason-

ló kártékony szoftver idéznek elő, potenciálisan a nem fegyveres, nem katonai fizikai erőszakalkalmazás köztes világának eszközei közül valók. Ez az értelmezés mindazonáltal elszakad nemzetközi jog azon gyakorlatától, hogy szigorúan csak az erőszak eszközeire fókuszál, mert a bevetett eszközök hatását is mérlegeli már. A hatást illetően azonban szigorú követelményeket fogalmaz meg: az erőszak alkalmazásának jelentékenynek, súlyosnak, tartósnak és messzire hatónak kell lennie, vagyis mértékét, hatótávolságát, intenzitását tekintve meg kell közelítenie egy fegyveres támadást (*scale and effect*). Hogy hagyományos hasonlattal éljünk: két állam fegyveres határvillongásai nem lépik át ezt a küszöböt. Martin van Creveld hadtörténészt egyszer már idéztük: „*War is killing*” – kell lenniük sebesülteknek és halottaknak. Az erőszaknak kárt tennie személyek testi épségében, össze kell kapcsolódnia emberélet elleni támadással – hatását robbanófej módjára kell kifejtenie. Egy hibrid támadásnak olyan hatást kell kifejtenie, amely összevethető egy kinetikus effektussal.

Valóban a tömegpusztító fegyver jellegével rendelkezik egy számítógépes program biztonsági rése, amint azt Brad Smith, a Microsoft pénzügyi vezetője a WannaCry esetében állítja? Csakugyan összehasonlíthatunk egy *Zero Day*t egy Tomahawk cirkálórakétával? Nem, egy komputerprogram biztonsági rése nem fegyver. A tömegpusztító fegyverről szóló narratíva nem több, mint hasonlat, mert a számítógépes programok biztonsági rései nem alkalmasak fegyvernek. Nem fejtenek ki fizikai hatást a számítógépekre, és embereket sem ölnek. Sem komputerekben,

sem személyekben nem tesznek kárt. Amíg nem használják ki őket kártékony programok, egyáltalán nem történik semmi.

S hogyan értékeljük azt a kártékony programot, amely egy biztonsági résen át behatol egy számítógépbe, adatokat lop, rombol, vagy lehetetlenné teszi a hozzáférést? Ez sem lép túl a megengedhető erőszak mértékén – keletkezzen bár mégoly nagy gazdasági kára annak, akinek a gépét megfertőzték.

Ugyanez a kérdés vetődik fel, amikor egy állam tartós jogosulatlan hozzáférést szerez a károsult állam rendszereihez. Ez az az eset, amely az amerikaiaknak álmatlan éjszakákat okoz: a mélyen az amerikai infrastruktúrákba ágyazódott orosz alvó programok, amelyek aktiválódása egyesegyedül Vlagyimir Putyin politikai akaratától függ. Mivel azonban az amerikaiak rendelkeznek csúcstechnológiai affinitással és technológiai jártassággal, és még a várható katasztrófa előtt sok időt, pénzt és munkát fektethetnek digitális védelmi vonalak kiépítésébe, az alvó programok önmagukban nem jelentik erőszak alkalmazását, és az önvédelemhez való jog sem juthat érvényre.

Maradnak azok a kártékony programok, amelyek (ipari) létesítményeket, például acélműveket, gáz- és kőolajvezetékeket vagy erőműveket oly módon vezérelnek, hogy ennek nyomán üzemzavarok keletkeznek – tehát a digitális szabotázs. Noha maga a kártékony program nem fegyver, mégis csak rendelkezik azzal a potenciállal, hogy a megzavart berendezést vagy létesítményt kvázi-fegyverként alkalmazza. Ha ugyanis felrobban egy megfertőzött vezérlésű gázvezeték, a létesítmény fizikailag tönkremegy; ennek során talán még embereknek is bajuk esik.

Alighanem a kritikus infrastruktúrák elleni, kártékony kód által végrehajtott súlyos szabotázs, aminek következtében emberek sokasága hal meg – a rettegett *digitális Pearl Harbor* – volna az egyetlen elképzelhető eset, amely összemérhető volna egy fegyveres támadás kinetikus hatásával. Az analógia mindenesetre hipotetikus, mert ilyen esetre a gyakorlatban eddig nem került sor.

A Stuxnet, a számítógépes féreg, amelyet feltételezhetően az Egyesült Államok és Izrael fejlesztett ki, és az iráni atomlétesítmények programozható logikai vezérlőibe csempésztett be, bizonyosan az erőszak tilalmába ütközne. Az akció során több mint ezer uráncentrifuga károsodott olyan súlyosan, hogy évekkel vetették vissza az iráni atomprogramot. Azért kell azonban feltételes módot használnunk, mert a Stuxnet-műveletről a nemzetközi közösség sosem tanácskozott. A nemzetközi jognak van ugyanis egy sajátossága. Ahogyan a német büntetőjogban az indítványra üldözendő bűncselekmény esetében is: egy államnak kifejezetten ki kell jelentenie, hogy egy másik állam a nemzetközi jogot megsértve megtámadta, csak akkor vált ki az eset nemzetközi jogi jogkövetkezményeket. Mármost Irán mindig is cáfolta, hogy kárt szenvedett volna. Soha nem panaszkodott, hogy hibrid támadás áldozata lett. Így aztán soha nem is vetődött fel a Stuxnet-támadás nemzetközi jogi megengedhetőségének kérdése.

És mi a helyzet a szűnni nem akaró szurkálásokkal, a napi tízmillió körüli digitális támadással, ami pergőtűz-szerűen zúdul a Deutsche Telekom AG és partnerei globális infrastruktúrá-

jára?^[37] Ha mindig ugyanattól a támadó államtól indul ki, és összegezzük, vajon az összes együttvéve átlépi-e a tiltott erőszak küszöbét?

Itt segíthet egy Izraellel való összevetés. Az országot folyamatos hagyományos támadások érik a Gázai-övezetből. Izrael számtalan alkalommal védte ki a palesztin Hamasz támadásait, bombázta a Gázai-övezetet, kitartva amellett, hogy joga van az önvédelemhez. A nemzetközi közösség kinyilvánította aggodalmát, ám tudomásul vette Izrael lépéseit. „Tiltott erőszak!” – kiálthatnák ezért a folyamatos digitális pergőtűzzel kapcsolatban is. Emellett még egy érv szól: ha egy agresszor folyamatosan zaklat valakit azzal a szándékkal, hogy tartósan és tudatosan megsértse a nemzetközi jogot, ő maga nem hivatkozhat a jogvédelemre, amit az erőszak tilalma biztosít számára, hanem tűrnie kell, hogy a sértett állam éljen megalapozott önvédelmi jogával.

Az agresszor keresése

„Először is, a cyber- és hibrid hadviselésben nem tudni pontosan, kik a szembenálló felek. Azonosítani kell a támadót, mielőtt megtorló intézkedésre kerülhet sor. Másodszor, mekkora az a kár, amelynél kimondható: »Ez nemzetközi jogba ütköző támadás volt. Háborúban állunk?« Természetesen a háborúban is vannak szabályok, de: *We can kill*. Hadviselőket meggyilkolhatunk. És ez legális.”^[38] Ezek Tobias Vestner nemzetközi jogász

szavai, egyáltalán nem szívesen halljuk, jogilag azonban helytálló, amit mond. Vestner közvetett módon utal egy központi fontosságú problémára: az olyan áldozat számára, aki nem tudja megállapítani, ki támadta meg, az önvédelemhez való jog írott malaszt.

A 20. században senkinek sem kellett feltennie a kérdést, hogy kitől indult ki a fegyveres támadás. Japán Pearl Harborban megtámadta az Egyesült Államokat, Németország megtámadta Lengyelországot, Líbia pedig Csádot. Kétség sem fért a támadó kilétéhez, és ki-ki inkább azzal foglalkozott, hogy miként és hol támadott az ellenség, hogy ezután felmérje a károkat, és megszabja a reakció mértékét.

A 21. században, amikor a kémkedés és a szabotázs digitális eszközökkel folyik, ez megváltozott. Mire egy hibrid támadás áldozata egyáltalán észleli a digitális infrastruktúrájában okozott kárt, sok idő telhet el, olykor egy egész évnél is több.^[39] Egy hibrid támadás pedig csak akkor jogosít fel az önvédelemre, ha azt az állam felségterületén kívülről, egy másik állam hajtja végre, ereje megfelel egy fegyveres támadásének, és a sértett állam mint ilyet rója fel. Ha azonban senkinek sem lehet felróni, nem lehet szó önvédelemről: elengedhetetlenül szükséges, hogy a támadást tulajdonítani lehessen valakinek.

Egyébként az, hogy egy digitális támadót nehéz egyértelműen azonosítani, megmagyarázza, miért nem történtek mindmáig súlyos, terrorindíttatású digitális támadások. A digitális kémkedést és szabotázst gyakran fedett műveletként hajtják végre. Erre egyenesen csábít az internet anonimitása; a tá-

madásokat tehát a legtöbb esetben tudatosan elleplezik, és nem akarják, hogy össze lehessen kapcsolni elkövetőkkel. Egy provokátor számára, aki ezzel szemben kifejezetten magára vállalna egy támadást, mert a világban félelmet és aggodalmat akar kelteni, problémát okoz a tettes azonosításának bonyolultsága. Egy sikeres digitális csapásra ugyanis más agresszorok, terrorcsoportok és más haszonlesők éppúgy igényt formálhatnak, mint a valódi elkövető. A nyilvánosság sokáig, sőt talán soha nem tudna biztosat arról, hogy a támadást valójában ki követte el. Tények, alternatív tények és összeesküvés-elméletek keringenek, és magának a támadónak okoznának kárt. Ekképpen szándékolatlan elrettentésre kerülhetne sor, mégpedig kifejezetten az online platformok és ezek társadalmi hatásai révén.

Egy további ok, amiért a terroristák nem hajtanak végre digitális támadásokat, hogy a lehetséges kár csekély nyilvános figyelmet kelt. Csak a digitális szabotázs legsúlyosabb esetei – mint egy repülőgép lezuhanása, aminek során emberek halnak meg, vagy egy atomreaktor zónaolvadása – gerjesztené a célul kitűzött rémületet a lakosság körében. Még mielőtt azonban egy számítógépes féreg, mint a Stuxnet, vagy pedig egy autonóm drón egyáltalán sikerrel tönkre tehetne létesítményeket, a támadónak sok pénzt és know-how-t kell a kártékony program létrehozásába fektetnie. És még ez sem elég: egy merénylőnek ismernie kell támadása célpontjának pontos műszaki részleteit. Ez csak akkor lehetséges, ha előzőleg (titkosszolgálati) felderítést végez. A terroristák ugyan igyekeznek kihasználni a meglepetés hatását – és csak az a meglepő, amivel senki sem számol –,

összességében azonban valószínűtlennek tűnik, hogy egy digitális támadásnak akkora hatása legyen, mint egy terroristák által végrehajtott fegyveres akciónak. Ez persze nem jelenti, hogy a konfliktuskezelőknek preventív terveikben ne kellene számolnia – legalábbis némi valószínűséggel – azzal, hogy egy szélsőséges digitális terrorakcióba kezd.

A helyzet akkor válik kényessé, ha technikailag már sikerült azonosítani az elkövetőt: immár diplomáciai, politikai bonyodalmak fenyegetnek. Mi következzen? A támadó megnevezése és megszégyenítése, *naming and shaming*? Érdemes nyilvánosan vállalni a vádak hangoztatásával és a cáfolatokkal járó hercehurcát, olyanformán, mint amikor a Kreml annektálta a Krímet, vagy amikor orosz exügynököket mérgeztek meg Nagy-Britanniában?

A nyilvános felelősségre vonás minden esetben súlyos diplomáciai következményekkel jár, ám ugyanilyen végzetes eltitkolni, hogy ki volt az elkövető, mert így az érintett lakosság továbbra sem sejt semmit. Nem tudja, hogy hibrid támadás érte, vagy hogy hamarosan ilyen éri majd. Tudatlanságban hagyják afelől, hogy stratégiai célponttá vált, s így senki sem készülhet fel az elképzelhetetlenre.

Ami a nemzetközi jog személyi alkalmazási feltételeit illeti, az mindenesetre bizonyos, hogy az agresszornak a nemzetközi jog alanyának, tehát egy másik államnak kell lennie. A támadás végrehajtásához az agresszornak nem szükséges saját fegyveres erőit igénybe vennie, alkalmazhat helyettesítőt is. A rajtaütéseket az állam magánzsoldosokhoz is kiszervezheti: egy digitális

Blackwaterhöz. Hamis azonosságú szereplőkhöz, egy idegen zászló alatt végrehajtandó hadművelet során.

Ha a hibrid támadást olyan helyettesítő hajtja végre, aki egy kormány megbízásából cselekszik, a megtámadott állam védekezése akkor is csak a nemzetközi jogi alany – tehát a támadó állam – ellen irányulhat. Maguk a privát zsoldosok nem alanyai a nemzetközi jognak, tényszerűen azonban a támadó állam hadviselőivé válnak. „*We can kill*. Hadviselőket meggyilkolhatunk. És ez legális.”

És még akkor is, ha az állam nem adott megbízást hibrid akcióra: magánszemélyeket bízott meg erőszak alkalmazására, ami olyan súlyossági fokot ér el, hogy egy állami katonai akcióval egyenértékű – a ma közkeletű meggyőződés szerint ez olyan fegyveres támadás, amellyel szemben a megtámadott államnak szabad védekeznie. 2001. szeptember 11-e óta ez a nemzetközi jogi gyakorlat.

Mindez még több kérdést vet fel. „Ajánlja-e fel az állam vállalkozásoknak szolgálatait egy *hack back*hez, ahogyan ez jelenleg Ausztráliában történik, vagy inkább a vállalatokat »hatalmazzák fel«, hogy maguk hajtsanak végre ilyen műveleteket, amiről többek közt az amerikai Kongresszusban folyik vita?”, veti fel a problémát Heiko Borchert biztonsági tanácsadó.

E kérdésekre olyasvalaki adhat választ, aki a nemzetközi jogból ugyanazokat a következtetéseket vonja le, mint például a „Tallini kézikönyv 2.0” szerzői az esetkommentárjaikban. A szakértők véleménye persze semmire sem kötelez jogilag. Két

példaként felhasznált tényállásból – ausztrál megközelítésben – a következő válaszok vezethetők le:

1. eset: Vállalatokat magánszereplők hekkelnek meg, akiket államok irányítanak, vagy akik egy állam megbízottjai:

A vélelmezett nemzetközi jogi (figyelem: nem büntetőjogi!) legitimitástámadások – egy másik állam hírszerzési, adatlopási, lélektani hadviselési és propaganda-akciói – esetén nem lép életbe a megtámadott állam önvédelemhez való joga. Ha azonban az érintett nemzetközijog-alany Ausztrál Nemzetközösség reakciója a támadásra *hack back* volna, az nem jogos önvédelemnek, hanem támadó intézkedésnek számítana, ami mint ilyen, a nemzetközi jogba ütközne – ha nem volna ugyanannyira legitim, mint az eredeti támadás.

Ha az állami agresszornak és magánszoldosainak hekkertámadása egyenértékű egy Ausztrália elleni fegyveres támadással, a nemzetközi jog alkalmazható; ilyenkor azonban a támadásnak egy fegyveres támadás hatásával és volumenével kell rendelkeznie, hogy érvénybe léptesse Ausztrália jogát az önvédelemre, ekkor azonban nem szükséges, hogy visszahekkelésre szorítkozzon. Csakhogy: ki az önvédelem címzettje? A támadó magán-delegáltjai bizonyosan nem, hiszen nem nemzetközijog-képesek. A védelmi intézkedésnek minden esetben az irányító állam ellen kell irányulnia, amelynek felelősséget kell vállalni szoldosainak offenzív magatartásáért.^[40] Minden esetben feltétel azonban, hogy a támadást egyértelműen fel lehessen róni egy államnak. Ha ez nem tehető meg teljes biztonsággal, Auszt-

rália számára csak az a lehetőség marad, hogy a hekkertámadásokat büntetőjogi úton üldözze.

2. eset: Vállalatokat nem államilag irányított magánszereplők hekkkelnek meg: Mivel sem a tettesek, sem az áldozatok nem alanyai a nemzetközi jognak, az nem is alkalmazható rájuk. Magánszemélyek vagy vállalatok magánszemélyek vagy vállalatok elleni hekkerakciója bűncselekmény, és a büntetőjog eszközeivel üldözhető. Ha azonban az Ausztrál Nemzetközösség felajánlja az érintett vállalkozásoknak a visszahekkkelést, az lehetővé teszi a nemzetközi jog alkalmazását, Ausztrália ugyanis eredeti nemzetközijog-alany.

A hack back, amit a nemzetközijog-alany Ausztrália hajt végre, akkor nem önvédelem, hanem támadó cselekmény, ami, ha nem esik a legitimitás-vélelem hatálya alá, vét a nemzetközi jog erőszaktilalma ellen. Támadó cselekményként Ausztráliának egy ilyen hekkertámadása érvénybe léptetheti a célállam önvédelemhez való jogát – annak összes következményével: állami szankciókkal, a gazdasági és nemzetközi kapcsolatok súlyos megromlásával és esetleges megtorló intézkedésekkel együtt. Itt és most túl messzire menne annak mérlegelése, vajon Ausztrália védekezhetne-e azzal, hogy mindössze magánmegbízatásból, nem pedig állami szuverenitása alapján, hanem maga is vállalkozóként járt el. Inkább feltételezzük, hogy az állam nem minden esetben léphet fel vállalkozóként, különösen nem olyanként, amely büntetőjogilag releváns tevékenységeket vállal. Hová is jutnánk...

A két példa nyomatékosítja, mennyire a józan ész parancsa, hogy a hibrid támadások esetében érvényesülő jogot is restriktíve értelmezzük, és hogy a visszahekkkelést csak a jogos önvédelem eseteiben alkalmazzuk. Ezért részesítette az ausztrál hírszerző szolgálat vezetője igen határozott figyelmeztetésben azokat az ausztrál cégeket, amelyek számára mind vonzóbbá válik a magán-*hacking back*. A jogellenes *hacking back*re adott olyan komoly politikai reakciók érkezhettek, hogy valamikor csakugyan sor kerülhet arra, amit senki nem akar: a forró háborúra.

Harmadik állam ellen egyébként soha nem szabad második csapást intézni. Hibrid cselekmények során harmadik államok tudtukon kívül eszközökké válhatnak, ahogyan a DNC elleni 2016-os hekkertámadások esetében, amikor támadó akciók előkészületeképpen harmadik államok területén béreltek szervereket. Egy ilyen visszaélés áldozatává lett harmadik államnak először jóvá kell hagynia, hogy felségterületéről önvédelmi műveletet kezdeményezzenek.

Foglaljuk össze: a hibrid támadás súlyának egy fegyveres támadásával összemérhetőnek kell lennie ahhoz, hogy érvénybe léptesse az önvédelem jogát. Ha a támadás nem tulajdonítható más államnak, a nemzetközi jog nem alkalmazható. A megengedett erőszak alkalmazását semmi sem támasztja alá, ez pedig annyit tesz, hogy: nincs *hack back*, nincs hagyományos második csapás, nem lehet szó nukleáris fegyver bevetéséről, nem alkalmazható a NATO-szerződés 5. cikkelye, nincs mód az ENSZ Biztonsági Tanácsának közreműködésére, nem érvényesíthetők kollektív állami büntetőintézkedések.

Nem marad más, mint a nemzeti bűnüldöző eljárás.^[41]

[ÖT]

Harc a dominanciáért

Külpolitikájában Kínát a félelemtől és részrehajlástól mentes mesterséges intelligencia segíti. (Stephan Chen)

„Vajon akar-e az USA a Közel-Kelet rendőre lenni úgy, hogy semmit sem kap érte, de értékes életeket és dollármilliárdokat áldoz mások megvédelmére érdekében, akik szinte soha nem ismerik el, amit teszünk? Mindörökre ott akarunk maradni? Itt az ideje, hogy végre mások harcoljanak...”^[1]

Az újabb kori történelemben nem először esik meg, hogy az Egyesült Államok visszahúzódik a világ történéseitől. Ismét egyedül önmagával akarja beérni – egy olyan pozícióval, amelyet elnöke a belpolitikában a siker legjobb kilátásaival képviselhet. Amerika ugyanis kényelmes helyzetben van: potenciálisan önellátó. Egy viszonylag kis lakosság a világ legnagyobb repülőhordozó-flottája birtokában él egy tekintélyes forrásokkal rendelkező, tágas szigeten, egy olyan remek szomszéd mellett, mint Kanada. Semmiben nem szenved hiányt, sem energiatartalékokban, sem a digitális korban szükséges tehetségekben. Végülis a Szilícium-völgy ezerszám gyűjtötte be az információtechnológiában legjobb szakemberek ezreit az egész világról. Geost-

ratégiai szempontból az Egyesült Államok mindenképpen a nyertesek közé tartozik. Most, hogy Donald Trump a Fehér Ház lakója, „az inga a neoizolacionizmus irányába leng ki”. Megengedhetik maguknak.

Miután az Egyesült Államok a Trump-adminisztráció alatt visszavonult, nem marad hatalmi vákuum utána. Oroszország geopolitikája lép a helyére, és egy még mindig alábecsült, globális vezető szerepre törő nagyhatalom, amelyet eddig egyáltalán nem vizsgáltunk: Kína, a Közép Birodalma.

Mindkét hatalom alkalmat ad Donald Trumpnak arra, hogy kiterjessze, újra kijelölje és biztosítsa majdani befolyási szféráját. Trump következetesen járt el, amikor 2018-ban az Egyesült Államok nemzeti biztonsági stratégiájának a *great power competition*, a nagyhatalmak versengése címet adta. Az új doktrínával Amerika háborúja a terror ellen a múlté lett. Helyére a nemzetek újabb fegyverkezési versenye lépett. Hajtóereje ennek is a katonai téren megszerzendő technológiai fölény iránti igény.

Hogy a Kreml miképpen akarja visszanyerni egykori nagyhatalmi státuszát, a hibrid hadviselés mestereként Oroszország 2014 óta a Krím-félszigeten, Kelet-Ukrajnában, illetve 2018-ban az Azovi-tengeren mutatta meg a világnak. Moszkva azt demonstrálja, hogyan kell semmibe venni a nemzetközi jogot és megsérteni az erőszak tilalmát anélkül, hogy komoly következményeket kellene elszenvednie – talán a nemzetközi közösség gazdasági szankcióin kívül, amelyek viszont hatástalanul enyésznek el. A moszkvai tőzsdén ugyanis hasonlóan jó vagy rossz az üzletmenet, mint Frankfurtban vagy New Yorkban,

mindenesetre nem szembeszökően rosszabb. A mezőgazdasági szankciók pedig, amelyeket Oroszország ellen a nemzetközi közösség az ukrajnai események után életbe léptetett, felszabadították az oroszok kreativitását. Az addig importált agrártermékeket saját, helyi produktumokkal helyettesítették, aminek az lett a következménye, hogy Oroszország a mezőgazdasági áruk egyik vezető exportőre lett. Új pozíciója köszönhető a gyenge rubelnek is. A 2018-as év folyamán az orosz deviza árfolyama a dollárhoz viszonyítva mindazonáltal 20 százalékkal lett magasabb.

Kína a térnyerés más taktikáit követi, mint Oroszország. Katonai téren földrajzi térségek lezárásával és hozzáférhetőségük korlátozásával operál. Így például manőverező robotrepülőgépeket állomásoztat a Dél-kínai-tengeren, vagy akadályozza az amerikai hadihajókat, amelyek ott nemzetközi vizeken tevékenykednek. Politikai síkon Kína feltűnő gyakorisággal avatkozik bele idegen kormányok ügyeibe. A harmadik államok belpolitikájába való beavatkozás eszközeihez tartozik bevándorló kínaiak megjelenése a belső piacon és a tudományos intézményrendszerben – az amerikai diákok 25 százaléka a matematikai, informatikai, természettudományi és technológiai szakokon kínai –, s ugyanígy a közvetlen beruházások a releváns technológiai cégekbe vagy a taktikailag fontos kikötők, repülőterek vagy szállítóútvonalak hitelfinanszírozásai Európában, a Közel-Keleten és Afrikában.

Pedig az Egyesült Államokat évtizedeken át elismerték globális rendfenntartó hatalomnak, mert minden tekintetben képes

volt érvényesíteni vezetői törekvéseit. Amerika vezető tengeri hatalom, légi hatalom és szárazföldi hatalom akart lenni, vezető szerepet vinni a gazdaságban és a világűrben, s már korán a „cybertérben” is. Ahol globális vezetési igényeinek érvényesítése csak katonailag volt lehetséges, ott az amerikaiak imperialisztikusan jártak el, és katonai támaszpontokat építettek, mint Afganisztánban vagy Irakban. Ha az USA a demokrácia magasabb rendű kultúráját és vele a szabad piacok eszméjét exportálta, hegemoniális hatalomként a *soft power*t alkalmazta.

Ez volt az a gazdasági és kulturális modell, amely mindennekelőtt az európaiakat is megnyerte. Azután, hogy 1941-ben az amerikai Augusta hadihajó fedélzetén, ahol a zöld asztal mellett Theodore Rooseveltt és Winston Churchill foglalt helyet, ütött a „a Nyugat születésének órája”,^[2] az Egyesült Államok jóformán ellentételezés nélkül bocsátott közjavakat csatlósállamai rendelkezésére: külső biztonságuk katonai védelmével vagy olyan szabadon hozzáférhető technológiákkal győzte meg őket, mint a *Global Positioning System* (GPS), illetve a mi kritikánk szempontjából lényeges internet és ennek platformjai. Az USA nagyszabású befektetésekkel úgyszintén biztosította magának globális hatalmi pozícióját, valamint más nyugati államok feltétel nélküli hűségét és lojalitását.

Amerika és a profit logikája

De ugyanez az amerikai jellegű globalizáció az oka annak is, hogy sokan úgy érzik, lehagyták őket. Az amerikai globalizáció az egész világra kiterjedő „átkapitalizálást” jelent, állapítja meg Ulrich Menzel, a nemzetközi kapcsolatok egyetemi tanára.^[3] A professor emeritus Kína kiváló ismerője, és évtizedek óta kíséri figyelemmel az országban folyó hatalmas áttörést. Azért hangsúlyozza az általunk ismert globalizáció amerikai jellegét, mert a globalizáció egészen máshogy is működhet, mint ahogyan mi ismerjük és tapasztaltuk:

„A globalizáció azonosítása a kapitalizmus egész világra való kiterjesztésével – éspedig neoliberais minta alapján – tévedés. A kínaiak a globalizáció más formáját gyakorolják.”^[4]

Vizsgáljuk meg alaposabban az amerikai eredetű globalizációt. Eltökélten kapitalisztikus lévén, vállalkozói szemléletű. Profitorientált.

„Ha a profit logikája szerint járok el, be kell fektessem a bevételek egy részét, hogy fokozzam a munka termelékenységét, és versenyképes maradjak a piacon. A profit logikája szerint a jövedelem forrása végső soron a magasabb versenyképesség.”^[5]

A versenyképesség növelése érdekében az áruk, a munkalehetőségek után költöző emberek, valamint a pénz nemzetközi áramlását úgy kell koordinálni, automatizálni és irányítani, hogy a költségek csökkenjenek, a profit pedig maximális legyen. Ez nem működik digitalizáció nélkül, ami a termelés és a szolgáltatás finanszírozásától a készpénz nélküli fizetésig optimalizálja az értéktermelés láncolatát. Az olyan digitális üzleti modell, amilyen az Amazon cégé, nem más, mint az áramlásszabá-

lyozásnak a logikai manifesztációja. Arra törekszik, hogy az értéktermelés teljes hálózatát kézben tartsa.

Világos, hogy azok az országok, amelyek nem rendelkeznek működő és biztonságos logisztikai infrastruktúrával – utakkal, kikötőkkel, vasúti pályákkal, repülőterekkel és megbízható digitális hálózatisággal –, kívül rekednek az átkapitalizálódáson. A globalizáció hosszú időn keresztül ezért korlátozódott az északi féltekére, az ipari országokra és néhány küszöbállamra. Az infrastruktúra nélküli afrikai országok többsége kimaradt belőle.

[6]

A kaliforniai Szilícium-völgy az információs kapitalizmussal bizonyos mértékig amerikai „Globalizáció 2.0-t” harangozott be.

[7] Digitális vállalkozásai húsz év óta gyűjtik az emberekről az adatokat, amelyeket nem törölnek. A kapitalizmus három virtuális javához, nevezetesen a munkához, a földhöz és a tőkéhez hozzácsatoltak egy negyediket is, amivel pénzt lehet keresni: az információt. A sokmilliárd ember által hátrahagyott adatnyomok alapján kiszámítják az egyének és a társadalom profilját és jövőbeli viselkedését, amit tovább értékesítenek, elsősorban hirdetőknak és ügynökségeiknek. A magasabb kattintásszámok az információs térben készpénzt jelentenek a digitális platformok számára, és további fogyasztásra, valamint növekedésre serkentik a gazdaságot. [8]

Pedig az információs kapitalizmusban megcélzott profit logikája nem olyan kézzelfogható javakon nyugszik, mint a föld vagy a munkateljesítmény, hanem nagy mértékben absztrakt javakon. [9] Noha a kapitalizmus már az 1970-es években elkezdett

leválni a reálgazdaságról, s először finánckapitalizmussá mutálódott, amelyben a pénznek kellett pénzt keresnie, de a kézzelfogható valóságtól a 21. században távolodott el még inkább, amikor a pénzkereset alapjává a testetlen adatok és információk lettek, és még több virtuális termék és szolgáltatás épült fel más, egyébként is már virtuális alapon. Az Apple iTunes milliós mikroszolgáltatást hozott létre, az appokat; a Facebook volt az alapja a fotoalkalmazásoknak; online játékokhoz tarka felületeket lehet vásárolni; a messenger-szolgáltatásokkal aláírás emoji-készletek járnak együtt, amelyeknek készítői szmájlijukat teli torokból ezzel a szlogennel reklámozzák: „Gigantikus előrelépés!”^[10] Ami egy tarka szimbólumokból álló gyűjteményben gigantikus, az legfeljebb a reklámlózung, éspedig a túlzás mértéktelenségét tekintve, az emoji-k ugyanis aligha juttatják el az emberiséget a Marsra és vissza, a Földre, ahogyan a klímakatasztrófát sem akadályozzák meg.

Mihelyt lehetőség adódik a pénzkeresetre, még egy jó ötlet is pervertálódik, akárcsak az internet. Tobzódásszámba megy, ahogyan a digitális gazdaság stimulálja magát, túlzást túlzásra halmoz. Nem mentesül ez alól a mesterséges intelligencia, és az értékek internetje sem a maga megosztott könyvelési technikájával, a blockchinnel, amelyet már „új mesterséges intelligenciaként”^[11] ünnepelnek. Aki pénzt akar keresni, annak nagy hangerővel kell felhívnia magára a figyelmet.

A neoliberalizmus térnyerése nem maradhatott következmények nélkül. Valahányszor valaki más törődik a dolgokkal, mi magunk elkényelmesedünk. Kerüljük a kockázatot, és oportu-

nista módon csak a kínálkozó alkalmakat ragadjuk üstökön. Mivel az Egyesült Államok és magántulajdonban lévő technológiai óriásai dollármilliárdokat fektetnek a digitalizációba, és a „digitális gyártási folyamatot” nagyrészt ingyenesen kínálják fel, első pillantásra gazdaságilag kevésbé tűnik észszerűnek, hogy pénzt fektessünk egy *Made in Europe* digitális infrastruktúrába. Csak a második pillantásra jövünk rá: mi magunk nem rendelkezünk digitális technológiákkal – másoktól függő viszonyba juttattuk magunkat. A német védelmi ipar ezt közben részben felismerte, és dolgozik termékei dezamerikanizálásán. Már nem szívesen vetjük alá magunkat az amerikai szoftvergigászoknak, ezek sűrű frissítési ciklusainak vagy licenszpolitikájának.^[12]

Az a sok éven át tartó tétovázás, ami az európai digitalizálási szándékokat kísérte, összevethető azzal, ahogyan Németország a katonai kiadásaival kapcsolatban eljár. Ulrich Menzel lényegre törően fogalmaz: „Visszahúzódtunk a potyautas pozíciójába: »Nem akarunk magas katonai kiadásokat. Arra költsenek az amerikaiak. Mi inkább szociálpolitikát csinálunk, és a civil ágazatokra összpontosítunk.« Hiszen nem kérdés: azokban is sikeresek vagyunk.”^[13]

Európa tehát potyázik, és nemcsak védelmi ügyekben. A rég begyakorlott opportunista mentalitás arra is magyarázattal szolgál, hogy kedvenc márkáink – az Amazontól a WhatsApp-ig – miért a Szilícium-völgyből, és miért nem Rómából, Stockholmból vagy Berlinből származnak. Az ugyanis, hogy előszeretettel használunk amerikai technológiát, nemzetközi kapcsolatainkkal függ össze. Most azonban kiderül, hogy Európa mégiscsak

óriási kockázat vállal, amikor olyan digitális kulcstechnológiákkal és üzleti modellekkel kapcsolatban, mint a felhő-szolgáltatók, a platformok vagy az ingyenesen rendelkezésre álló mesterségesintelligencia-könyvtárak, Amerika-függővé tette magát. A Szilícium-völgy csillaga ugyanis közben már rég nem ragyog oly fényesen, mint egykor.

Minderről azok az informatikai hadműveletek is tehetnek, amelyeket az oroszok a 2016-os amerikai elnökválasztási kampány idején hajtottak végre. A digitális platformok gazdái nemcsak parlamentek előtt kénytelenek számot adni antidemokratiкус törekvéseikről, hanem civil panaszok is érkeznek címükre. Platformjaik társadalmi kockázatait illetően nincsenek válaszaik, és ami még rosszabb, régóta elhárítanak mindenféle társadalmi felelősséget. Végülis, mondhatják, profitorientált vállalatok, nem úgy működnek, mint az Üdvhadsereg.

Miközben azonban maguk a törvényhozók is messzemenően adósok maradnak a digitális platformok társadalmi problémájára adandó válasszal, és a területet csak töredékesen szabályozzák, befektetőik következetesen büntetik az információtechnológiai ipar legnagyobbjait, a *Big Techet*: a Google a 2018-as évben tőzsdei értékének körülbelül 25 százalékát veszítette el, az Apple-nél a veszteség 40, a Facebooknál mintegy 50 százalékra rúgott. Ettől az európaiak is feleszméltek – amire már a Szilícium-völgy főnökei sem legyinthetnek a szokásos göggel. Mozgásba lendültek.

Elvont gazdasági javakkal profitot termelni, amelyek mindössze más elvont digitális termékeken alapulnak: a rendszerbe

kódolt jelentős kockázattal jár. Amikor új piacok nyílnak meg, illetve adatok és információk jelentette versenyelőnyök kínálkoznak, a gazdaság egy résztvevője egymagában csak akkor tud hatékonyan tevékenykedni, ha integrálódik a digitális gazdaság nagy egészébe. Más piaci résztvevőkkel szövetkezve dolgozik, vagy mások digitális teljesítményére épít. A hálózatiság, az adatfolyamhoz való akadálytalan hozzáférés és a zökkenőmentes kommunikáció nélkül gazdasági növekedés ma már alig lehetséges. Ezzel kapcsolatban a problémát az jelenti, hogy az euroatlanti civil digitális infrastruktúrát békeidőkre teremtették meg. Nem számol zavarokkal. Megszakítások nincsenek beleszámítva. Arra hagyatkozunk, hogy az internet mindig hozzáférhető, a sávszélesség pedig mindenkor zavartalanul áll rendelkezésünkre. Nagyszerű is, amikor ez a békegazdaság akadálytalanul működik. Mégis stratégiai hanyagság, ha csak a digitalizáció gazdasági előnyeivel számolunk, és nem gondolunk a digitális technológiák geostratégiai jelentőségére.

Pedig a stratégiaalkotásra való képtelenség a vakfolt Európa és speciálisan Németország szemében. Ha egy másik államból először egy ország digitális infrastruktúrája ellen intéznek nemlineáris támadást, a gazdaság és az ipar hosszú időre elveszítheti azokat a beruházásait, amelyeket egy békebeli digitális infrastruktúrában valósított meg. Másként fogalmazva: ha a profitlogikája a hálózatiság zavartalan működésére hagyatkozik, mihelyt a geopolitikai helyzet változik – hogy azt ne mondjuk: rosszabbodik –, a digitalizálásba való beruházások tévedések-

nek bizonyulhatnak. A helyzet ma erőteljesen szembesíti a világot ezzel a kényelmetlen ténnyel.

A középhatalmaknak, amilyen Európa, ma arra kell berendezkedniük, hogy az Egyesült Államok visszahúzódása az „Amerika Erődbe” tovább fokozza más államok – mindenekelőtt Oroszország és Kína – hibrid lépéseinek valószínűségét. A két rivális ugyanis, amely a világuralomért vetélkedik Amerikával, megtartja, megszilárdítja, sőt ki is terjeszti majd hatalmát. A 21. században a rég meghaladottnak gondolt világhatalmi politika sajnos ismét fellendülést él át. Kína a globális fölényt, Moszkva régi hatalmának restaurálását célozza meg.

Kína rendszeralternatívája: a járadék logikája

Valójában Kína az, akitől a digitalizáció következő hullámát várhatjuk. A népköztársaság már régóta nem éri be azzal, hogy másolja az amerikaiakat, kivéve persze egyvalamit: a birodalmi hatalomra való törekvést.

Különösen a Kína által exportált hatalmi rendszer különbözik alapvetően az amerikai globalizációtól. Ulrich Menzel szemléletesen így írja le a különbséget:

„A világ nagy részében nem a profit, hanem a járadék logikáját látjuk működni, és a járadékrendszer globalizálódik. Az antitézis tehát így hangzik: a globalizáció nem a neoliberális értelemben vett kapitalizmus, hanem a járadékalapú rendszerek el-

terjedését jelenti. E téren Kína, Oroszországhoz hasonlóan, élvás.”^[14] A profit, fűzi hozzá az egyértelműség kedvéért a professzor, a tőkebefektetések megtérítése, a bér az emberi munka díjazása, a járadék pedig a földhasználat hozadéka.

„Miközben a föld mindazt jelenti, ami a föld alatt található. Tehát nemcsak a mezőgazdaságot, hanem a bányászatot is.”^[15] És kőolajat. Marihuánát. Gyémántokat, vizet, területeket. Aki ezt vagy azt kitermel és megművel, nem profitérdekelt vállalkozóként cselekszik, hanem járadékot húz.^[16]

Ha akarjuk, ebből arra következtethetünk, hogy Donald Trump egyáltalán nem vállalkozó. Ingatlanjai használatát harmadik feleknek engedi át, akik ezért lakbérrel vagy bérleti díjjal tartoznak neki. Ezáltal Trump járadékélvezője ingatlanvagyonának, éppúgy, mint a szaúdi-arábiai olajsejkek, akik olajkészleteiket járadékjövedelmekké alakítják át.

A két jövedelmi modellnek olyan következményei vannak a majdani világrendre nézve, amelyeket csak lassan fogunk fel. Az euroatlanti rendszer digitális termelési folyamatban, absztrakt, testetlen nyersanyagokkal – adatokkal és információkkal – folytatott vállalkozói tevékenység során termel profitot, ugyanakkor egy rendkívül sebezhető virtuális, békebeli infrastruktúrát épít fel, és az információs fölényre alapozza versenyképességét. Kína és Oroszország másként jár el. „Nem vállalkozói tevékenységből, hanem gazdaságilag releváns források feletti politikai ellenőrzésből tesznek szert jövedelemre.”^[17] Vagyis a földből és mindabból, ami összefügg vele.

És ez a rendszer tartósnak bizonyul.

„A járadékjövedelmek előretörőben vannak, mert végső soron politikai hatalmon alapulnak – állapítja meg Ulrich Menzel. – Arra is magyarázatul szolgálnak, miért nem fejlődik ki a profit logikája sok országban. A járadék logikája erősebbnek bizonyul a profiténál.”^[18]

Még Donald Trump is felismerte a két modell különböző voltát: „Kína a nagy hegy [Afganisztán] másik oldala. Markolókkal van jelen [Afganisztánban], amelyek ásványokat termelnek ki; mi harcolunk, ők [a kínaiak] ásványokat visznek magukkal (...)”, állapította meg helyesen Trump már a 2015-ös választási kampány idején.^[19] A járadék logikájából ugyanis következik, hogy az ember földet is kisajátít magának. Kína ezt különösen látványosan teszi *land grabbing*, azaz nagyarányú földvásárlás útján Afrikában, vagy az Új Selyemút segítségével: tengeri folyosója Velencében ér véget, szárazföldi folyosója Duisburgon át Rotterdamig vezet.

„Az Új Selyemút-kezdemenyezés ugyanis nem az, amit egyesek Németországban hisznek, nem szentimentális emlékezés Marco Polóra”, figyelmeztetett ezért teljes joggal Sigmar Gabriel német külügyminiszter – szintén Ulrich Menzeltől inspirálva – a 2018-as müncheni biztonsági értekezleten.^[20] „Annak a kísérletnek a megjelenítője, hogy megalapozzon egy átfogó rendszert a világ Kína érdekei szerinti alakítására. Ennek során már korántsem csak a gazdaságról van szó: „Kína a nyugati berendezkedés átfogó rendszeralternatíváját építi, amely a mi modellünkkel ellentétben nem szabadságon, demokrácián és egyéni emberi jogokon alapul.”^[21]

Kína tehát nem az absztrakt javakat és a digitális gyártási folyamatot részesíti előnyben, mint az euroatlanti rendszer, hanem valami olyan kézzelfogható dolgot, mint a föld. Hogy mennyire fontos a népköztársaság számára a birodalmi magatartás és a területszerzés, kifejezésre jut abban a fenyegetésben is, amely kormánya részéről Tajvant, ezt a demokratikus ipari államot éri. A szigetet, úgymond, egyesíteni kell a szárazfölddel, ha szükséges, katonai erő alkalmazásával is. S az ország, amely robotot küld a Holdra, hogy kiderítse, vajon üvegházi körülmények közt lehetséges-e ott zöldségek és virágok termesztése vagy selyemhernyók tenyésztése^[22], sohasem látott módon expanzív *land grabbinget* folytat.

A földet, amelyet valaki ellenőrizni akar, biztosítani kell. A biztosítás – és ez igen fontos vizsgálódásunk szempontjából – történhet katonai úton, kínai katonai támaszpontok építésével, amelyek gyorsan közelednek, ahogy a kínai tengeri haditámaszpont esetében Dzsibutiban, vagy határozott politikai számításon alapuló technológia-alkalmazással.

„E logika [ti. a járadéké] szerint a járadék egy részét szükségképpen a hatalmi apparátusba kell fektetnem. Azaz a rendőrségbe, a titkosszolgálatba, a hadseregbe, a különböző elnöki gárdákba, hogy – és ez a lényeg – biztosítsam a hatalmat a járadékot biztosító források felett”, mondja Ulrich Menzel.^[23] „A járadékbevételek egy részét újra meg újra a politikai kontroll fenntartására kell elkölteni. És nemcsak helyben, hanem ha a járadék logikája globalizálódik, másutt is.”^[24]

Azaz külföldön. A profitorientált nyugati rendszer feletti kontroll egyébként pénzzel is kitűnően megvalósítható. A 2015/17-es években a kínaiak közvetlen befektetései „háborút eldöntő” technológiákat gyártó hadiipari vállalkozásokba az összes kockázatitőke-tranzakció 10–16 százalékát tették ki. Ha ugyanis a pénz az, ami a nyugati információs technológiát működteti a maga digitális javaival, az adatokkal és információkkal, a befektetett összegek tervszerű kivonása, a dezinvestíció a legrosszabb esetben előidézhetheti ennek az információs gazdaságnak az összeomlását. Az adat még a digitális érában sem ugyanaz, mint a kőolaj vagy az arany. Aki a maga számára kőolajat, aranyat vagy bármilyen ásványi kincset biztosított, s egyidejűleg olyan helyzetbe hozza magát, hogy megszakíthassa vagy megállíthassa a nem anyagi jellegű nyugati javak áramlását, kényelmesebb pozícióban van, mint aki adattömegekkel rendelkezik, amelyek szó szerint kifolyhatnak ujjai közül.

Hogy a belföldi kontroll hogyan fest, Kína digitális társadalmi kreditrendszere illusztrálja. Az adatok, párosítva a mesterséges intelligencia kiértékelő kapacitásával, lehetővé teszik az összes kínai „jó állampolgárookra” és „rossz állampolgárookra” osztását, s ezzel a kínai nép feletti neototalitárius uralmat. Embertelen rendszer – így látja a Nyugat a tapasztalatok birtokában, amelyekre a zsidókat és fogyatékosokat milliószámra diszkrimináló és gyilkoló nemzetiszocializmussal kapcsolatban tett szert.

A kínai rezsim mindenekelőtt azért neototalitárius, mert nincsen rá szüksége, hogy az államapparátus tekintélyét a né-

pesség erőszakos nevelésével érje el. A 21. században az erőszak helyébe a mindenütt jelenlévő megfigyelési technológia lép. A fizikai erőszak alkalmazását társadalmi és gazdasági előnyök alkotta jutalmazási-büntetési rendszer váltja fel, amely egy-egy személy engedelmességére vagy engedetlenségére reagál. A digitális haladás lehetővé teszi az emberek erőszakmentes elnyomását. Az erőszak azonban nem tűnik el, hanem radikális megoldássá válik. A háború sem tűnik el, hanem helyette természetessé válnak az erőszakküszöb alatti hibrid támadások. Hipotézisünk úgy hangzik: az államközi konfliktusok a jövőben a két nagyon különböző rendszer összeütközése ellenére több erőszak helyett kevesebb erőszakhoz vezethetnek.

A magatartásmódosítás digitalizáció révén egyébként olyan igény, amelyet a New York-i x.ai vállalat is megfogalmaz: *Using Artificial Intelligence to program humans to behave better.*^[25] Az embert eszerint mesterséges intelligenciának kellene átprogramoznia, hogy jobban viselkedjen. A viselkedés módosítása egyeseknek profitot, másoknak kontrollt hoz. A célok különbözők, de a digitális eszközök ugyanazok.

Ha a digitális viselkedésmodifikáció még inkább elterjed és meghonosodik, valaha szabad államok nem túl rózsás időknek néznek elébe hosszú távon. Elnyomás áldozata lesz a demokrácia, az egyéni és az interszubjektív emberi jogok, a sajtószabadság vagy a vallásszabadság. Kína azonban a digitális technológiákat mégsem csak visszaélések elkövetésére alkalmazza, ahogyan ezt Európában gyakorta hallani. Ehelyett két nagyon különböző rendszer kelt nyílt versenyre egymással: a profit logiká-

ja és a járadék logikája, az amerikai átkapitalizálás és a kínai megoldás. Csak éppen Kína meg van győződve a maga rendszerre fölényéről. Az euroatlanti rendszer egyáltalán nem ilyen biztos a maga logikájában, s ezzel megkérdőjelezi saját korábbi öntudatosságát. Van azonban valami, ami közös a két rendszerben: egyik sem mondhat le a digitalizációról, jóllehet mindkettő számára más jelentőséggel bír. Az egyik oldal piaci eszközként használja, a másik a hatalom megtartásának eszközeként.

A putyinizáció: Make Russia great again

Ha az orosz rubel dollárra való átváltásának hivatalos árfolyamát vesszük alapul, Oroszország éves gazdasági teljesítménye a maga 1578 ezer milliárd dollárjával nem nagyobb New York államénál, és az USA bruttó hazai termékének mindössze körülbelül nyolc százalékát teszi ki (2017).^[26] Vásárlóerő-paritáson (VEP) számítva Oroszország bruttó hazai összterméke mindazonáltal több mint két és félszer magasabb.^[27] Ugyanez feltételezhető az orosz katonai költségvetésről is. Ha hiszünk a Stockholmi Nemzetközi Békekutató Intézetnek (SIPRI), az orosz katonai költségvetés nem sokkal magasabb, mint az amerikai védelmi költségvetés jó egytizede. Abszolút számokban kifejezve Vlagyimir Putyin eszerint a 2017-es évben 66,3 milliárd dollárt (VEP-en számítva: 168,7 milliárd dollárt) költött fegyverkezési céljaira, míg az Egyesült Államok 610 milliárd dollárt (2018-ban 710

milliárd dollárt, ami körülbelül 15 milliárddal több, mint 2017-ben).^[28]

Ulrich Menzel azonban szkeptikus, és felteszi a jogos kérdést: mi számít tulajdonképpen katonai kiadásnak. Az államoknak mindemellett nyugdíjakat is kell fizetni a veteránoknak, s ezek az Egyesült Államokban lényegesen magasabbak, mint Oroszországban. Valószínűleg ugyanez igaz a katonai illetményre is. Vajon beleszámolták-e a katonai kutatást, vagy sem? Közben az erre szánt amerikai költségvetés gyorsan olvad, Oroszországnak ehhez képest több dollárja marad, amit volta-képpen hadiipari termékeire költhet.

Az efféle aszimmetria miatt nehéz kiszámítani, valójában mekkora részét teszi ki egy ország védelmi költségvetése bruttó nemzeti össztermékének. Ami az USA-t illeti, az arány a 2017-es évben 3,14 százalék körül volt.^[29] Ehhez képest a német katonai kiadások 2017-ben 44,3 milliárd dollárt tettek ki, a bruttó nemzeti össztermék 1,2 százalékát. 2023-ig állítólag elérik majd az 1,6 százalékos szintet, és a körülbelül 60 milliárd eurót. Ezek szerint Németország a jövőben névleg ugyanannyit fektet majd a védelembe, mint ma Oroszország, ahol ez a kvóta – az összes említett fenntartással együtt – 2017-ben számszakilag nagyjából 4,2 százalék lehetett, ténylegesen azonban valószínűleg magasabb volt, ha tekintetbe vesszük a vásárlóerő-paritást.

A jókora különbség miatt, ami az orosz fegyverarzenálnak az utóbbi években végbement megfiatalodása és a Bundeswehr állapota közt fennáll – amelynek bevetési készségét a védelmi megbízottak, legutóbb 2019-ben, tartósan rossznak ítélték –, fel-

vetődik a kérdés, mire költi védelmi költségvetését Németország. Nyugdíjakra, akárcsak a többi állam is. Óvodai és napközi férőhelyekre meg lapos televíziókra a körletekben. Egy maroknyi fregatt felszerelésére, amelyek dízelmotorjainak meg kell felelniük az Euro5-ös vagy Euro6-os kipufogógáz-előírásoknak. Légszűrőkre a Leopard harckocsikba, amelyek zárt belső terére vonatkozik a meg nem született élet érdekében hozott finompor-szabályozás (magában a harckocsiban, nem azon kívül). Mindez alapvetően jó, és semmi sem szól ellene. Oroszországnak esze ágában sincs effélékre költeni. Annak láttán azonban, hogy az agyonbürokratizált német közigazgatási apparátust privát tanácsadócégek veszik körül, amelyeket – nehogy szabálytalanságokra kerüljön sor – más privát tanácsadócégeknek kell ellenőrizniük, már gondterheltebben sandítunk az olyan államokra, mint Oroszország, ahol a költségvetést nyilvánvalóan szívesebben fordítják a harcérték fokozására.

Oroszország a járadék logikáját követi, és olaj-, illetve gázkészletei exportjából él. Ebből azonban az orosz lakosság legnagyobb része nem profitál. Az ország legértékesebb állami üzeleinek, az orosz energiacégeknek a privatizációja ugyanis az 1990-es években meglehetősen balul ütött ki: csak egy oligarchaelitet tett gazdag orosz.

Az orosz kormány 1992-ben nagyszabású privatizációs program keretében kuponokat osztott ki az orosz népesség körében. Ezek bemutatása ellenében a lakosság részesedéseket szerezhett orosz üzemekben, köztük olyanokban, amelyek világméretben a legnagyobb energiaforrásokkal rendelkeztek. Az álla-

mi vagyon magánemberek közti, kisrészvények formájában való kiosztásával az volt a cél, hogy egy nyugati mintákat követő, piacorientált rendszer létrejöttét tegye lehetővé. A dolognak azonban több bökkenője is volt. Hogyan is mondta Ulrich Menzel? „A járadék logikája erősebbnek bizonyul a profiténál.”

Az oroszok többsége nem értette, mit kezdjen az értékjegyekkel, amelyeket Borisz Jelcin kormányától kapott. Sokan nem tudták felmérni a tényleges értéküket. Mindenesetre úgy vették, csak egy 30 dollár névértékű papírdarab van a kezükben. Szívesen belementek, hogy tömény italért vagy hét dollár értékű élelmiszerért – kicsalják tőlük a kuponokat. Ha egy leleményes szatócs felismerte, hogy a kuponokat felárral adhatja tovább, az összeset olcsón összevásárolta a falujában, és darabonként tizenkét dollárért továbbadta egy nagykereskedőnek. Ez utóbbi tízezres paketteket állított össze – darabját 18 dollárra taksálta – és eladásra kínálta a moszkvai kuponbörzén, a legprimitívebb értelemben vett tőzsdén, ahol kempingasztalokon kötegszámra adták-vették a kuponokat készpénzért.^[30] A vásárló amerikai dollárral fizetett, és jogot nyert arra, hogy résztulajdonosa legyen egy volt orosz állami üzemnek. A kormány egyébként nem tett különbséget, hogy a vevő orosz volt, vagy külföldi befektető. Egyébként ha állami orosz üzemek kerülnek a saját népesség osztott tulajdonában, az is kezdettől fogva a privatizáció politikai hibája lett volna.

Amikor a kuponok már rendelkeztek bizonyos értékkel – mivel beruházási javakra lehetett váltani őket –, még értékesebbnek számítottak, ha valaki orosz vállalatokban való részesedés-

re cserélhette be őket, amelyeket valós piaci értékük töredékére áraztak be. Nem 20 vagy 30 százalékkal, nem – hanem 90–99 százalékkal kevesebbre.^[31] Az orosz energiacégek értéke némi fáradsággal kideríthető volt; egy termelőüzem energiakészlet-számaait beszerezve következtetni lehetett arra, hogy tisztességes áron vajon mennyi volna a vállalat értéke, összevetve egy nyugati vetélytársáéval, például az Exxon Mobile-éval vagy a British Petroleuméval (BP). Így pár millió dollárért sokmilliárdos vállalkozásokban lehetett részesedéseket vásárolni.

A rendszerváltás éveinek káosza után az orosz vállalatokat végül már piacképes áron adták-vették. A kis számú résztulajdonos öröme. Első befektetésük ezerszeresét keresték meg, szöges ellentétben az orosz lakosság többségével, amely a *Szerencsés János* című Grimm-mese hőiséhez hasonlóan kétes csereügyletek során adta ki a kezéből az aranyrögöt.

Az orosz nemzeti vagyonnak az 1990-es években történt újraelosztása után Oroszország gazdasági elitjei összeolvadtak az ország politikai elitjével, hogy elkerüljék a sorsot, amely – elretentő példaként – Oroszország egykori leggazdagabb emberét, Mihail Hodorkovszkijt érte utol. Az oligarcha, aki a Jukosz nevű orosz olajipari óriást vezette, nem érte be a gazdasági hatalommal, és beszállt a nyílt hatalmi harcba Moszkvával. Letartóztatása, büntetőpere és elítélése nem váratott soká magára. A gazdaság más mágnásai megijedtek, és levonták az eset tanulságait: a politika csak azt hagyja békén, s csak az számíthat arra, hogy megtarthatja vagyonát, aki a kormány számára elfogadható módon viselkedik – a lehető legrosszabb előfeltétele volt ez az or-

szág nyugati jellegű piacgazdaságra való átállításának. Moszkva kézben tartotta oligarcháit, akik ezért Kreml-hű magatartást tanúsítottak, hogy a kormány ennek fejében érintetlenül hagyja a vagyonukat. A gazdasági és politikai elitek közti kompromisszum révén létrejött egy „thugokrácia”, egy maffiaszerű rendszer az állam irányításában részt vevő, valamint az állam által kontrollált csoportokból. Más nem állami, civiltársadalmi érdekközösségeket, amelyek kivonták magukat Moszkva kontrollja alól, rendszerellenes ügynökökké nyilvánítottak, és ellenséggént üldözték őket.

A balul sikerült privatizáció után Oroszországnak a Nyugathoz való közeledése meghiúsult, a járadékrendszer ellenben sikeresen meghonosodott. Az orosz hatóságok módszerei a továbbiakban elriasztották a külföldi befektetőket, az orosz gazdaság pedig nem fejlődött. A profit logikája ugyanis feltételezi, hogy egy ország egy gazdaságipolitikai modellt kedvező befektetői környezettel, vállalkozói magatartással és innovációkészséggel támogasson.^[32]

Oroszország azonban más úton indult el. Aggodalmában, hogy a nép az elit rablótempója és a gazdasági pangás miatt forradalmi megmozdulásokra ragadtatja magát – amilyen 2011-ben az arab tavasz vagy 2014-ben a kijevi Majdan téri események voltak –, és megdönti a moszkvai kormányt, 2012-es újraválasztása után Vlagyimir Putyin erőteljesebben fordult a nyilvánosság felé, és ösztönözni kezdte az orosz restaurációt. Az „Oroszország, az elismert nagyhatalom” narratíváját jó adag nacionalista mitológiával alapozta meg. Nyugatellenes érzelmeket

szított és emlékeztetett országának történelmileg elismert birodalmi törekvéseire – amelynek imperialista elődjét, a Szovjetuniót hermetikusan fal zárta el a Nyugattól 1989-ig: a hegemonia és az impérium éles elkülönítésének szimbólumaként.

Az ismét megerősödő világhatalom igényeiből – de a járadék makacsul stabil logikájából is – Moszkva azután levezette saját orosz technológiastratégiáját. Oroszországnak ugyanis, tekintettel korlátozott gazdasági teljesítményére és szűkös költségvetésére, nagyon pontosan át kell gondolnia, hogy milyen technológiákba akar befektetni, és ha a technológia ugrásszerű fejlődése behozhatatlannak látszik, hogy hogyan legyen kreatív. Pénzügyileg Oroszország nem engedhet meg magának annyit, mint az Egyesült Államok, ezért bizonyítottan a katonai szektornak kell előre vinnie a technológiai innovációt, aminek katonailag hasznosíthatónak kell lennie, mert a járadék logikája megköveteli a politikai és gazdasági kontrollt.

Az azonban, hogy a költségvetés szűk, nem jelent sokat, mert a 21. században a gazdagság nem okvetlenül korrelál a politikai vagy katonai sikerrel. A gazdaságilag gyenge országok mindig folyamodhatnak az aszimmetrikus konfliktus eszközeihez. Oroszország ezért is dolgozott azon, hogy a hibrid eljárások mestere legyen, ezért fejlesztette tökélyre a hadviselés nemlineáris jellegét. Az amerikaiak tudni vélik, hogy Vlagyimir Putyin fenntart legalább egy olyan irányítóközpontot, amely más államok környezeti intelligenciájában képes digitális hadműveleteket – legyen az digitális hírszerzés vagy szabotázs – végrehajtani: egymással koordinált és szorosan összehangolt informatikai

támadások és elektronikus hadviselés útján. Oroszország 250 ezer mobilantennát akar felállítani, s nem azért, hogy jobb internet-hozzáférést biztosítson lakosai számára, hanem hogy optimalizálja az elektronikus hadviselést és zavarja a globális műholdas navigációt.^[33] Rövid időközönként pedig kiderül, hogy az oroszok hibrid támadást indítottak nyugati környezeti intelligencia ellen. Egyidejűleg aláássák a megtámadott államok morálját: a dezinformációs kampányok az információs térben szociális zavarokat, társadalmi ellentéteket és félelmet idéznek elő.

Az is Oroszország technológiai stratégiájának része, hogy befogadja a technikai tekintetben tehetséges bűnelkövetőket. Ezek online kémkedést folytatnak, hírszerzési vagy katonai szempontból fontos adatokat és információkat lopnak, és online befolyásolási akciókkal politikailag olyan helyszíneken avatkoznak be, mint Ukrajna, Törökország, az USA, vagy az európai államok. Ha külföldön vádat emelnek ellenük, ahogyan ezt Robert Mueller különleges ügyész meg meri tenni, sőt le is tartóztatják őket, az orosz kormány minden eszközzel küzd szabadon bocsátásukért – már csak azért is, mert soraikból a Kreml majdani kormánytagokat rekrutál.^[34]

A hibrid képességek azonban önmagukban nem elégítik ki Moszkva ambícióit. A Kreml, hogy régi erejének is hasznát vegye, következetesen korszerűsíti atomarzenálját, amellyel az ország már a hidegháború idején is sikeresen fenyegetett. Pénzeiket fektetnek többszörös hangsebességű támadófegyverekbe, amelyeket egyaránt felszerelhetnek konvencionális és nukleáris robbanótöltettel. Nyugaton sokakat fog el az idegesség, mert az

ilyen hiperszonikus siklók pusztító sebessége is már meghaladja a fenyegetett államok védelmi képességeit. Megrendítik a stratégiai erőegyensúlyt; ezért diszruptív fegyvertechnológiaként „tűzveszélyesek”. S még ha Vlagyimir Putyin egy napon azt hangozza is be, hogy 2019-től üzembe helyez egy hangsebesség-nél 27-szer gyorsabb hiperszonikus fegyvert, röviddel utána pedig fegyverkezési költségvetésének megkurtítását jelenti be, egy modernizált orosz haderő technológiai képességeit nem szabad alábecsülni. Történetileg tekintve Oroszországnak vannak tapasztalatai a csúcstechnológiával. Az ISS nemzetközi űrállomás vagy a nemzetközi magfúziós projekt a dél-franciaországi Cadarache-ban még ma is profitál ebből. A fegyverzeti technológia olcsó előállítására tehát nem kell, hogy szükségképpen hatásosságának rovására menjen.

Ezt bizonyítja, illetve erősíti meg Oroszország ember nélküli rendszereivel, a katonai robotokkal. Kisebbség, olcsóbbak, egyszerűbbek, mint amerikai megfelelőik, és ha elvesztik őket a csatateret – például Szíria – felett, nem okoz túl nagy fejfájást. Megterveztek és már tesztelnek ember nélküli mini tengeralattjárókat, amelyek rajokban tevékenykednek, és mesterséges intelligencia segítségével koordinálják magukat, s ugyanígy autonóm mélytengeri műveletekre képes platformokat is. A nemzetközi vizek ellenőrzése lesz a feladatuk.

A mesterséges intelligencia vezérelte harci drónokra Moszkva egyelőre csak áhítozik. Itt nyilvánul meg az Oroszország és Amerika technológiai stratégiája közti egyik különbség. Az Egyesült Államok ember nélküli rendszereket alkalmaz, hogy

fokozza humán harcosainak képességeit. Oroszország tekintete előtt viszont az lebeg, hogy ember nélküli rendszerei katonái előtt vagy mellett teljesen autonóm bevetésre induljanak. Az oroszok hadműveleti koncepciója elég közel esik a LAWS-okkal kapcsolatos vízióhoz. Ennek ellenére kijelenthető, hogy az autokratikus rendszerek ragaszkodnak ellenőrzési paranoiájukhoz. De hogy a csatatér és az emberek megölése feletti ellenőrzést is átengedik-e egy potenciálisan kontrollálhatatlan gépnek, egyelőre még nyitott kérdés.

Azzal immár aligha kell számolnunk, hogy Oroszországban gyors demokratizálódás vagy liberalizálódás megy végbe. A történelmi Nyugat egységének hiánya a nyugati átkapitalizálódást nem teszi éppen vonzó rendszeralternatívává. Oroszország ezért is hozott létre más partneri kapcsolatokat. Elfordult Európától Kína felé, amelynek növekedési tervei szinte csillapíthatatlan energiaéhséggel járnak együtt. Mindazonáltal a kínai közvetlen befektetések aránya Oroszországban az EU-államokéinak mindössze az egyötvenedét tették ki 2017 közepén.^{[35],[36]} A Távol-Kelettel való együttműködés feltételezhetően nem úgy alakul, ahogyan Moszkva reméli. Az ok: Kínának megvannak a maga tervei.

A kínai álom

2013. március 14-én Hszi Csin-ping szerzi meg a Kínai Népköztársaság államelnöki tisztét. Hszi úr barátságos, joviális benyo-

mást kelt, ebből azonban tévedés lenne azt a következtetést levonni, hogy nem kormányoz majd erős kézzel, és hogy nem vonul majd be ugyanúgy a történelembe, mint Mao Ce-tung. Uralma alatt, amelyet öt évvel hivatalba lépése után, 2018 márciusában élete végéig meghosszabbítottak, Kína nem akar többé a nyugati kolonializmus áldozata lenni. Az ópiumháborúk és a boxerlázadás ugyan már több mint száz éve a múlté, ám abban a narratívában, amelyet a kormány a lakosságnak közvetít, föl lehet eleveníteni a régi traumát, hogy ébren tartsák a bizalmatlanságot.

Az euroatlanti rendszer egyelőre csak lassan fogja fel, milyen messzire jutott Kína az új technológiák fejlesztésében. Hszi Csin-ping 2030-ig csúcspozícióra akar szert tenni a mesterséges intelligencia területén, 2049-ben, a Kínai Népköztársaság megalapításának 100. évfordulóján pedig az ország, úgy is, mint a legerősebb gazdasági és katonai hatalom, fel akarja váltani az Egyesült Államokat a globális rendfenntartó hatalom szerepében. Saját holdutazási programon dolgozik, műholdakat, köztük kéműholdakat épít, a világ legnagyobb hadseregét mondhatja magáénak, saját repülőgépeket állít elő, illetve kínai repülőhordozó-flottát tart fenn. Közelebbről még nem ismert, mekkora Kína tengeri hadereje. Bruttóregisztertonnában mérve azonban az ország régen a világ legnagyobb hajóépítőjévé lépett elő.

[37]

Kína felemelkedése feltartóztathatatatlannak tűnik. „Valamikor a fenti időablakban [2030–2035] a kínai nemzeti össztermék felülmúlja majd az amerikaiét. A Kínára vonatkozó prognózisok

mindeddig inkább előbb, mint utóbb teljesedtek be”, kommentálja röviden és tömören Ulrich Menzel a kínai haladást.^[38]

Pedig Hszi nem mást akar, mint megváltoztatni a globális kormányzási rendszert.^[39] A történelem során első ízben konfrontálódik a világ egy kommunista jellegű bürokratikus fejlődő ország globalizációjával. Az új társadalommodell ugyanis, amelyet Hszi Csin-ping követ, nem demokratikus-kapitalisztikus. Hszi is egy olyan párt utópista politikáját képviseli, amely egymaga tart igényt az igazságra; a párttal és annak élén karizmatikus vezetőjével a kínai államkapitalizmus kihívást intéz majd a világhoz, mégpedig egy olyan, vaskézzel kormányzó autokrata irányítása alatt, aki egy egyöntetűre formált társadalmat akar vezetni, ellenzék nélkül, a párt irányításával. A cél az, hogy Kínával a középpontban egy nagy, globális család jöjjön létre, amelyben mindenki ugyanazt a jólétet, ugyanazt a biztonságot és ugyanazt a boldogságot élvezi. Hszi Csin-ping így nevezi ideológiáját: „a kínai álom”. Mindenki gazdag és sikeres lesz. A gazdasági fejlődés felvirágzik, csak épp demokratikus eszmék és nyugati értékek nélkül.

A biztonságról a gazdaság ütőere, az Új Selyemút mentén katonai erő alkalmazásával Kína gondoskodik majd, s e célból már most beavatkozik más országok belpolitikájába, oly módon, ahogyan erre Oroszország már példát szolgáltatott a 2016-os amerikai elnökválasztásokba való beavatkozással. Kína új világrendjét a geostratégia, a gazdasági stratégia, a külföldi politikai beavatkozás és politikai-katonai szövetségek ötvözete alkotja. Nem, a kommunista Szovjetunió 1991-es bukása Francis Fuku-

yama politikatudós egykori megállapításával ellentétben nem jelentette a történelem végét. Ezzel világpolitikai szempontból már rég nem érthetünk egyet. A sárkány felkelt, és hódító hadjáratra indult. Létrehozta a Sanghaji Biztonsági Szervezetet, a G7 kínai ellenpárját, és a 16+1 együttműködést – amelyben egyetlen ország, Kína vezet egy 16 európai államból álló koalíciót –, lehasítja a kelet-európai államokat az Európai Unió régebbi magjáról, s Albániától Magyarorszáig arra készíti őket, hogy Kína-barát, egyidejűleg pedig EU-kritikus álláspontot tegyenek magukévá.

A kínai álomért is nagy társadalmi árat kell majd fizetni, ugyanúgy, ahogyan ez már a Szilícium-völgy-ideológiák világ-méretű elterjedése esetében volt, és amelyekkel kapcsolatban csak a politikai sorsfordulót jelentő 2016-os év óta, lassanként válik nyilvánvalóvá, hogy miként és miért vallanak kudarcot. A kommunizmus történetének ismeretében hamar rájöhethetünk, milyen árat kell majd fizetnünk újbóli elterjedéséért. Nem más forog kockán, mint a *conditio humana*, az emberi létállapot. Kína kommunista pártjának ideológiája minden máshoz, az egyénhez képest is előnyt kell élveznie. Az embereket feláldozzák az „egésznek”. Egyetlen személy mit sem számít. Mindenkinek alá kell rendelnie magát a kínai álomnak. Az elhajlókat nem fogják megtérni. Aki mégis ellenáll, attól könnyű megszabadulni. Ez a mindenkori kommunista felfogás: „Az individuum nulla; az individuum semmi. A párt: minden.”^[40] Az ember nem személy, aki szabadságjogokat élvez, hanem csak egy atom a társadalmi rendben, tárgy, amit nem illetnek meg saját jogok.

Hszi Csin-ping, aki ezen a módon szocializálódott, a *9-es számú dokumentumban*, egy stratégiai tervezetben, amely angol fordításban 2013 óta olvasható, megtiltotta, hogy országában szó es-
sék hét témáról, köztük az egyetemes emberi jogokról, a demok-
ráciáról, a szabad újságírásról és a civil társadalomról.^[41] Ezek
tiltott, ellenséges eszmék. Mindegyik árt Kína terveinek.

Kína geopolitikai ambícióit kielégítendő Hszi Csin-ping stra-
tégiai paktumot kötött a digitalizációval. Különösen a mestersé-
ges intelligencia alkalmazásától remél geostratégiai és katonai
előnyöket. Ellentétben az euroatlanti rendszerrel, amely gazda-
sági és társadalmi összefüggésekben gondolkodik, Hszi össze-
kapcsolja Kína bel- és külpolitikáját nemzete technológiai fejlő-
désével, a civil és a katonai szféra egyesítését pedig a kínai tech-
nológiai gigászoknak a politikába és a katonai ügyekbe való szo-
ros bevonásával valósítja meg.^[42] Ez egy egészen másmilyen
technológia-stratégiához vezet, mint amelyet a nyugati modell
követ – már amennyire az egyáltalán kialakított valamilyen ko-
herens stratégiát.

A Nyugat csak lassan fogja fel, hogy Kína mekkora stratégiai
kihívás elé állítja. A kínai kormány digitális koncepcióinak meg-
lepően erőteljes, politikailag és katonailag motivált fejlődését a
nyugati demokráciák sürgősen utol akarják érni. Ennek ellené-
re például a német kormány 2018 novemberében született,
„Mesterségesintelligencia-stratégia” című dokumentuma a leg-
kevésbé sem veszi tekintetbe a mesterséges intelligenciának
mint univerzális technológiának a geostratégiai relevanciáját,
ami olyannyira központi jelentőségű viszont az olyan járadék-

alapú országok jövője szempontjából, mint Kína vagy Oroszország. A német liberálisok is szeretnék távoltage magukat a technológia-stratégiától, s átengedni a gazdaságban tevékenykedő mérnököknek: ők szívesen dolgoznak rajta. Washingtonban viszont felfigyeltek arra, hogy a szó szoros értelmében talajt veszítenek Kínával szemben. Erről pedig az amerikai átkapitalizáltság is tehet. A technológia és az innováció túlságosan a piacokhoz igazodik – és túl kevésbé a biztonsághoz és a politikához.

Szingularitás a csatatéren

Aszerint, hogy egy ország a profit vagy a járadék logikáját követi, a technológia-stratégiák is eltérnek egymástól. Kína, amely a történelmi Nyugattól eltérően a természeti erőforrásokat igyekszik megszerezni, a járadék logikájából más digitális stratégiákat vezet le, mint a libertárius digitális kapitalisták.

„A járadék logikája feltételezi a politikai ellenőrzés megtartását”, hangsúlyozza a politikatudós Ulrich Menzel.^[43] Így aztán logikus, hogy a digitális technológiáknak, különösen a mesterséges intelligenciának ilyen hatalmi garanciákkal kell szolgálniuk, és inkább geostratégiai és katonai előnyöket, semmint vállalkozói versenyelőnyt kell biztosítaniuk. Ezt a következőképpen kell elképzelünk: az Új Selyemút kezdeményezésben 70 ország vesz részt, ily módon tehát a világ teljes lakosságának mintegy 65 százalékát érinti. Kínát már a terv nagyságrendje is rendkí-

vüli külpolitikai kihívások elé állítja. Ahhoz, hogy Peking az Új Selyemút mentén politikai hatalmat fejthessen ki, új befolyási szféráját Velencéig és Rotterdამig kell bebiztosítania.^[44] Ehhez hozzátartozik az is, hogy Kínának szavatolnia kell az Új Selyemút tengeri és szárazföldi útvonalainak biztonságát; a kínai katonai támaszpontok egyre nyugatabbra tolódnak. Ulrich Menzelnek nincsenek kétségei:

„Tengeri úton? Megoldják!”^[45] A kínaiak legalábbis már hozzáláttak egy repülőhordozó-flotta felépítéséhez. A nemzetközi kapcsolatok szakértője azonban abban már kételkedik, hogy az olyan országokban is képesek lesznek gondoskodni a szárazföldi útvonal biztonságáról, mint Afganisztán vagy Üzbegisztán.^[46]

Mintha csak neki akarnának ellentmondani, a kínai Népi Felszabadító Hadsereg titkos kutatólaboratóriumokban lázasan kutatja, hogyan tehetne szert „technológiai szingularitásra a csatatéren”.^[47] A mesterséges intelligenciának átfogó katonai biztonságot kell teremtenie, hiszen óriási fölényben van a humán katonákkal szemben, de legalábbis emberfeletti gyorsaságú döntésekkel, a katonai összecsapások során pedig lendületesebb tempó biztosításával támogatja ember-bajtársait. A kínai stratégia újdonságát tehát a mesterséges intelligencia alkalmazási doktrínája jelenti, ez (ti. a mesterséges intelligencia) az, ami egyáltalán megvalósíthatóvá teszi a kínai neokolonializmust, valamint a digitális technológiáknak a kínai álom magasabb céljára való, kifejezetten erőteljes stratégiai összpontosítását.

Kína következetesen halad előre, a mesterséges intelligenciát mint kulcstechnológiát egyre több, biztonsági szempontból rele-

váns alkalmazásban igyekszik felhasználni, ennek ellenére (még) nem állja meg a helyét, hogy a NATO-államok technológiai téren lemaradásban volnának mögötte.

A NATO-államok a mesterséges intelligenciát már az 1990-es évek vége óta használják katonai helyzetképek számítástechnikai kidolgozására. A nyugati modellnek azonban Kínával kapcsolatban egészen egyértelműen van egy stratégiai problémája. Jóllehet a Szilícium-völgyben, az amerikai keleti parton, egyidejűleg pedig Európában – Nagy-Britanniában, Franciaországban és Németországban – támogatnak és szorgalmazznak digitális projekteket, ezek azonban nem integráns részei egy nemzeti vagy európai össz-stratégiának. Tény, hogy a digitalizáció – az elektronikusan felfegyverzett *Homo superior* eszméjétől a gazdasági növekedés iránti igényig – számos ideológiát akar kiszolgálni: „A három [német] kulcságazat a járműgyártás, a gépgyártás és a vegyipar. Ezekben muszáj az élen maradni. Az autónak számítógéppé kell válnia. Már nem a gépészmérnökre, hanem az informatikusra vagy az elektrotechnikusra hárul a döntő feladat”, vélekedik Menzel Németországgal kapcsolatban.^[48]

A feltörekvő Kína nagyhatalmi szándékait látva azonban kevés volna, ha a digitalizációban mindössze egy jobban teljesítő gazdaság hajtóerejét látnánk. A profit logikája különben is csak akkor valósítható meg, ha biztosítva van az átdigitalizált társadalom békéje és biztonsága. Ennek digitalizációs erőfeszítéseit azonban veszély fenyegeti, ha nem kerül sor az adott ország digitális képességeinek újraértékelésére: először is, a mondott készségek között szerepelnie kell, hogy meg tudják határozni a

hibrid támadások értelmi szerzőit, képesek legyenek útját állni digitális hozzáférési kísérleteknek, és hogy nemzetközi platformokon is vonzó demokratikus narratívákat tudjanak előadni. Másodszor, és ezt nem lehet elégszer hangsúlyozni, be kell ágyazódniuk egy saját európai biztonsági érdekeket kifejező, koherens össz-stratégiába.

A járadék mint technológiai királycsináló

	A PROFIT LOGIKÁJA	A JÁRADÉK LOGIKÁJA
KÉPVISELŐI	USA, Európa	Kína, Oroszország
A LOGIKA CÉLJA	versenyképesség, a verseny új területeinek feltárása, gazdasági növekedés	térnyerés, térbiztosítás, politi- kai kontroll
VILÁGKÉP	vállalkozói-libertárius	államilag irányított
DIGITÁLIS STRATÉGIÁK CÉLJA	Információs dominancia: <ul style="list-style-type: none"> • felhasználói profilok digitális kinyerése • magatartásmódosítászárt kibernetikai szabályzókörben való megfigyelés útján 	Hadszintéri szingularitás: <ul style="list-style-type: none"> • (bel)politikai irányítás és kontroll, pl. közösségi jutalompont-rendszer útján • a politika és a haderők technológiai fölénye
KULCS- TECHNOLÓ- GIA*	Mesterséges intelligencia	Mesterséges intelligencia
KULCS- TECHNOLÓ- GIA PRIMER ALKALMAZÁ- SI KONTEXTU- SAI	Automatizálás: <ul style="list-style-type: none"> • adatgyűjtés, adatelemzés • predikció (prognózis), pl. eladási számoké, fogyasztói viselkedése 	Autonómia: <ul style="list-style-type: none"> • adatgyűjtés, adatelemzés • információs hadviselés irányítása

	<p>ajánlórendszerek, pl. TMK-hoz</p> <ul style="list-style-type: none"> • digitális asszisztensek • emberi munka automatizálása pl. call centerben, az értékteremtési láncolatban, robotizált folyamatautomatizálásként 	<ul style="list-style-type: none"> • okos parancsnoki rendszerek • autonóm (humanoid) robotok és drónok • szimulációs rendszerek • képzési/kiképzési rendszerek • döntéstámogatás • komplex dinamikus (emergens) rendszerek • hibrid intelligencia, pl. ember-gép-kooperáció
--	---	---

** További kulcstechnológiák, amelyeket Kína intenzíven kutat: idegtudományok, kvantumkommunikáció, genomszerkesztés és pénzügyi technológiák.*

[HAT]

„Csak feltételesen védekezésre
kész”

A 21. század világában ugyanis csak a béke, a biztonság és a külső stabilitás iránti közös elkötelezettség révén vívható ki Európa békéje. És mivel most egy biztonsági konferencián veszünk részt, nyilván azt is jelenti, hogy a demokráciáknak mindig egyensúlyt kell tartaniuk nem katonai és katonai tűrőképesség között. (Sigmar Gabriel)

Mike Tyson, az amerikai ökölvívó-legenda olyan kisugárzással rendelkezett, hogy az megfélemlítően hatott embertársaira. Ő nem pusztán legyőzni akarta ellenfeleit, azt szerette volna, ha már első ökölcsapása *megöli* őket – és ebből nem is csinált titkot. Zsenge 13 éves korára már 38 őrizetbe vételen volt túl, sportsikerei ellenére súlyos drog- és alkoholproblémákkal küzdött, jogerősen elítélték nemi erőszakért, és másodjára is börtönbe került, amikor egy bokszmérkőzés során, amelyben vesztesre állt, leharapta kihívója, Evander Holyfield fél fülét. Egyszer egy riporter arról kérdezte, mi a taktikája fürge lábú, gyors ellenfe-

lekkal szemben, ő pedig ezzel az elhíresült mondattal felelt: „Mindenkinek van egy terve, amíg nem kap egyet a pofájára”.

Donald Trump sincsen valami nagy véleménnyel a tervezésről – ezt Mike Tyson barátjától tanulta, akinek 1988-tól díjazás ellenében üzleti és bírósági ügyekben tanácsokat adott. A tervezés felesleges, jelentette ki Trump frusztrált tanácsadói előtt a Fehér Házban, s mintegy ennek megerősítéseképpen Tysonnak épp az említett mondatát idézte, amely ma az összes internetes idézetgyűjteménynek ékessége. Az elnök ahelyett, hogy politikai célokat tűzne ki maga elé, impulzív módon cselekszik. Még a tanácskozások előkészítését is feleslegesnek tartja.^[1] A helyzetek állandóan változnak, az embernek újra meg újra ringbe kell szállnia minden nap – hangzik Trump jelmondata.^[2]

„Szó szerint lehetetlen előre látni, nem változtatja-e meg a véleményét egyik pillanatról a másikra”, árulta el a sajtónak egy névtelen partizán az Ovális Irodában.^[3] Olykor ugyan esetleg kijelenti, hogy van valamilyen terve, az azonban, mint mondja, titkos. Akár nem létezik terv, akár titkos a terv: a közönség mindkét esetben számosat nem ismer a konkrét célok közül, amelyeket elnöke kitűz maga elé, s amelyekhez Trump politikai előrehaladását lehetne mérni – leszámítva a Mexikó és az USA közti határfal építésének előrehaladtát. Bármelyik technológiai startup-vállalkozás többet tervez, mint Washington.

Donald Trumptól eltérően Hszi Csin-ping rendelkezik egy rendkívül nagyratörő politikai céllal, és mindent-mindenkit „kínai álma” megvalósítására sorakoztat fel. Természetesen Hszi-nek is küzdenie kell a bizonytalansággal: a kínai gazdaságot ke-

reskedelmi háborúk vetik vissza, a növekedési adatokat esetleg kozmetikázzák, egy ekkora népesség csak nehezen kontrollálható, a kínai Népi Felszabadító Hadsereg nem korszerűsödik a kívánt gyorsasággal. Hszi terveinek a stratégiai következetesség kölcsönöz nagy lendületet, akkor is, ha globális szinten a környezet dinamikusan és előre nem látható módon változik. Ilyenkor utólagos szabályzásra van szükség, anélkül azonban, hogy a magasabb rendű célt szem előtt tévesztenék. Még egy mesterséges neurális hálózat is rendelkezik célfunkcióval.

Kína célirányosan jár el a viláგuralomért folyó versenyben, és ugyanígy tesz – még ha más dimenziókban is – Oroszország. Donald Trump ezzel szemben mindössze az Amerika Erődbe való visszavonulásra törekszik, „konzervatív izolacionizmusra, amin szélsőséges változatában az összes külső káros befolyás kivédését és a világ konfliktusaiba való be nem avatkozást (...) érti.”^[4]Amerika a saját határain belüli protekcionista önelégültség mellett döntött, amit a kínai álm visszاسzorítására tett intézkedésekkel köt össze, de csakis a saját hasznát nézve. Az Egyesült Államokból Kínába irányuló technológia-transzfert az amerikai cégekbe való külföldi közvetlen befektetések állami korlátozásai és a digitális technológiák exportjának ellenőrzése hivatottak megakadályozni.

Frontvonalban

Ott, ahol a két rendszeralternatíva földrajzilag ütközik, geostratégiai törés keletkezik. Egy képzetes tengely, a nyugati törésvonal mentén, amely északon Ukrajnától Szírián, Izraelen és a Gázai-övezeten át délen Jemenig húzódik, a két logika harca olyan rendkívüli eseményekben jut kifejezésre, amelyek túlmennek a hibrid fenyegetéseken. Itt forró háborúk zajlanak. Európa, amely nyugaton közvetlenül határos a geostratégiai törésvonallal, nemcsak a térszomszédságában zajló katonai erőszak következményeit érzi meg. Ha ez a vonal tovább tolódik nyugat felé, mivel a kínai modell Európára is áttérjed – márpedig erre sok minden utal –, a konfliktusok még kontinensünk közepét is eluralhatják.

Európától nyugatra már senki sincsen, aki segítő kezet nyújtana. Keleten zátonyra futott nukleáris egyezmények, hightech-fegyverkezés és nagyhatalmi törekvések fenyegető kulisszái tornyosulnak fel. És a képletes rendszertörésvonal közelében ott fekszik Európa, az az Unió, amely alapítása óta először érzi szükségét a stratégiai autonómiának.

Az egykor egységes Nyugat nem várhat sokat Donald Trump Amerikájától: ő már nem törekszik a demokrácia és a neoliberális globalis exportjára, és többé ezek biztonságáról sem kíván gondoskodni. A NATO-ból való kilépésről és a Világkereskedelmi Unióból való kiválásról twitterezik, elhagyta az ENSZ Emberi Jogi Bizottságát, és elrendelte az amerikai csapatok kivonását Szíriából, ami az afganisztáni csapatkivonást is valószínűbbé teszi. Külügyminisztere, Mike Pompeo pedig nyilvánosan és nem éppen diplomatikusan kétségbe vonja, hogy az Eu-

rópai Unió még mindig polgárainak érdekeit szolgálja. A Brexit, úgymond, ébresztő volt. Azokat a nemzetközi szervezeteket, amelyek már semmivel sem járulnak hozzá az együttműködés fejlesztéséhez, meg kellene reformálni vagy fel kellene oszlatni – így Pompeo.^[5]

Amerika visszavonulása azt jelzi, hogy a hatalom a világon többé nem egyetlen pólusba összpontosul, hanem átadja helyét egy multipoláris berendezkedésnek. Kína csillaga gyorsan emelkedik. Afrika sokféle potenciállal rendelkezik, de ki van téve az éghajlatváltozás következményeinek, s ráadásul gyilkos vallási fanatikus csoportok jelenlétével szembesül, amelyek a kontinens egyes részeit olyannyira bizonytalanná teszik, hogy az afrikai életkörülmények javulására alig van remény. Az Atlanti-óceán túlsó partján Latin-Amerika jelentős részei követik a járadék logikáját. Számos dél-amerikai államban korrupció és állami szintű válság uralkodik. Venezuela labda Oroszország és Amerika mérkőzésén, Argentínában az infláció majdnem 50 százalék, Brazília pedig elnökké választotta a maga Donald Trumpját, Jair Bolsanarót. A politikai helyzet csak Ázsiában tűnik viszonylag nyugodtnak. Japán az amerikanizáció képviselői közé tartozik, India pedig a világ legnagyobb – noha működési zavarokkal küszködő – demokráciája.

Kínának a gazdasági növekedés és a szigorú politikai kontroll révén egyelőre sikerül fenntartania a stabilitást és biztosítani a lakosság elégedettségét, ennek ellenére a Távol-Keleten is létezik egy rendszerek közötti árok: annak a nyugati geostratégiai törésvonalnak a megfelelője, amely Oroszország nyugati

határa mentén a Közép-Keletig húzódik: a Csendes-óceáni törésvonal, amely északon a Koreai-félszigeten kezdődik, és Tajvanon át a Dél-kínai-tengerig tart. A szárazföldön található Kína, a Csendes-óceán térségében Japán, Óceánia, Ausztrália és az amerikai nyugati part. Az azonban, hogy az USA a geostratégiai törésvonalak mentén katonai kötelezettségeket vállal, fegyverkezik és a Távol-Keleten repülőgép-hordozókat állomásoztat, egyáltalán nem mond ellene az ismét megerősödött amerikai izolacionizmusnak, hanem annak a jele, hogy a 21. század világrendjéről e vonalak mentén születik majd meg a döntés. Miközben Kína saját stratégiájával tökéletes összhangban sérti meg a nemzetközi jogot, vagy egyébként is illegálisan jár el – mert például megfenyegeti a Fülöp-szigetek kormányát arra az esetre, ha az áram előállítására céljából az óceánon akarna földgázt kitermelni –, az Egyesült Államok még megpróbálja fenntartani a régi rendet.

Európa is válságban van, és minden, csak nem egységes. Nagy-Britannia úgy döntött, hogy kilép az Unióból, s a továbbiakban egymagában áll. A keleti bővítés országai alig rendelkeznek integratív erővel, és az illiberális demokrácia koncepciójával, a sajtószabadság és a független igazságszolgáltatás korlátozásával magukat az Unió politikai alappilléreit támadják. Skandinávia, amely a világ tökéletes demokráciáinak listáján előkelő helyet foglal el, speciális eset, meglehetősen higgadt és legtöbbször sikeres a szociális érdekek kezelésében. Egy negyedik európai régiót alkot az ún. Mag-Európa, amely az Unió alapeszméjének értelmében továbbra is még békésen, egységesen, vagy leg-

alábbis kompromisszumokra készen akar együtt élni, nem mentes azonban a szociális feszültségektől és társadalmi megosztottságtól. Franciaországban a sárgamellényesek demonstrálnak a reformok ellen, egész Európában előretörőben van a jobboldali populizmus, a digitalizáció pedig súlyos szociális gondokkal fenyeget azokon a helyeken, ahol a munkát automatizálják, vagy pedig a technika gyorsabban terjed, hogysen az emberek megtanulhatnak, hogyan bánjanak vele.

Az erők belső és külső dinamikája közepette Európának valamilyen jövővízióra van szüksége.

Utazás cél nélkül

Európa már a 19. század közepén egyensúlyi politikát folytatott, amelynek eszközét a szövetségekben találta meg. Míg a világ egypólusú, az álláspontok és a szövetségesi partneri viszonyok gyorsan tisztázódnak, egy multipoláris rendben ez nem így van. Az opportunizmusnak, a haszonlesésnek és a tényleges fölénynek vége. Tartósnak hitt kapcsolatok szűnnek meg, politikai megrázkódtatások arra kényszerítenek államokat, hogy önállóan folytassanak világpolitikát.

„Tény, hogy az Európai Uniót és elődjét, az Európai Gazdasági Közösséget nem arra szánták, hogy képes legyen világpolitika folytatására. Sokáig nem voltunk világpolitika-képesek. A körülmények hozzák magukkal, hogy törekednünk kell erre”, állapította meg egy 2018-as beszédében – helyesen – Jean-Claude Juncker, aki hosszú éveken át volt az Európai Bizottság elnöke.

Üzenete nem jutott el mindenkihez. A nyugati gazdaság és politika a jövőben is a profit logikája szerint akar működni. A geostratégiai szempontokat szívesen elhanyagolják, különösen a gazdaság és az ipar. Érzékelik ugyan, hogy a piacok mindinkább átpolitizálódnak, a növekvő kockázatokat azonban adottként veszik tudomásul. Ahogyan eddig, úgy most is minden erőfeszítésük a versenyképességre és a gazdasági növekedésre irányul, még a világnak azokon a részein is, ahol a járadék logikája uralkodik. Jóllehet az Oroszországhoz fűződő viszonyt gazdasági szankciók terhelik meg, Kína egyértelműen az európai gazdasági növekedés mozgatórugójának számít. Ez a körülmény nem tűr politikai feszültségeket. Csak nagyon visszafogottan hangzik el, hogy a kínai modell a gazdasági kérdéseken messze túlmutató problémákat is magában rejt.

Amennyire széthúzó Európa a maga egészében, annyira koordinálatlanok még azok az erők is, amelyek kitartóan a profit logikáját követik. Csak Németország is több bizottságot állított fel, és jónéhány önálló stratégiát dolgozott ki, amelyek a digitalizációval foglalkoznak, s amelyek céljai részben átfedik egymást: abban, hogy értéket jelentenek a gazdaság számára, jövővízióval szolgálnak az iparnak, és új piacok új igényeit tárják fel.

Ha valamiben, hát testületekben, papírban, és így felismerésekben nincs hiány. Digitális stratégia, mesterségesintelligencia-stratégia, cyberbiztonsági stratégia, offenzív cyberképességek... csak kár, hogy az anyagi és szellemi erőfeszítések, amelyek ahhoz szükségesek, hogy a jövő technológiájában is vezető szerepünk legyen, nem integrálódnak hosszútávú, ambiciózus politi-

kai programokba, amelyek egy majdani Európa víziójához igazodnak. A versenyképesség megőrzésén kívül Európa eddig nem tűzött ki magasabb rendű célt – épp az a világpolitikai igyekezet várat magára, amit Jean-Claude Juncker kívánatosnak tartott. A versenyképesség azonban egymaga aligha tud majd bármit is szembeállítani azzal a kínai rendszerlogikával, amely nem éri be a társadalmi együttélés normaminimumaival, hanem globális magatartási kódexet akar érvényre juttatni. Ami hiányzik, az az egyértelmű európai pozíció, és a szándék, hogy a politikai vízió érdekében is új technológiákat vessünk be. Aki nem hajlandó a perspektívaváltásra – mert ez nem illik bele a diskurzus beszűkült terébe, és nem egyeztethető össze a következő növekedési hullám alternatívátlanásával –, nem lesz képes helytállni a rendszerek versenyében.

Bátorság a határozott demokráciapolitikához

Európának világpolitikai vízióra van szüksége. Természetesen megteheti, hogy ennek megtalálása érdekében szemügyre veszi politikai, katonai, technológiai, jogi és gazdasági arzenálját, és felteszi a kérdést: vajon mindezzel mit érhetnek el az európaiak? A német diskurzus során gyakran felvetődő egyik lehetséges válasz sarkítva így hangzik: „Iparunk és tudományunk viszi előre az új technológiákat, amelyek nagyszerű, modern jövőt alakítanak ki.” A németek úgy gondolják, az új technológiák olyan nyomást fejtenek ki a társadalomra, hogy az változni kénytelen; nem arra várnak, hogy a társadalom megváltozzon,

és aztán új technológiákat igényeljen, hogy jobban megszervezhesse magát. A társadalmat szerintük a tudósok és mérnökök technológiai innovációinak kell átformálnia, ami voltaképpen egyszer már végbement, amikor az Apple cég 2007-től elárasztotta a földgolyót okostelefonokkal. Azóta sok minden megváltozott. Az emberek máshogyan kommunikálnak, máshogyan dolgoznak, másként szeretnek és élnek, mint azelőtt.

Ám az is csak egy narratíva, hogy erről a társadalmi diszkontinuitásról tudósok és mérnökök döntöttek. Ami első ránézésre határtalan kutatási és fejlesztési szabadságnak tűnik, másodikkra csak opportunizmus. A tudósok és mérnökök ténylegesen már semmit sem maguk döntenek el. A befektetők teszik meg helyettük, az investorok, akik maradéktalanul elkötelezték magukat a profit logikája mellett. A „tudomány mint a gazdaság táskahordozója” és a professzor átalakulása „tudósból tudományos munkássá”^[6] jóval inkább megfelel a valóságnak, mint az az elképzelés, amely szerint a tudósok és mérnökök azon dolgoznak, hogy egy nagyszerű jövőt tegyenek lehetővé a társadalom számára.

Praktikusabb fordítva felszerszámozni a lovat, és először az európai álmot megálmodni. A „Milyennek képzeljük az eljövendő Európát?” kérdés a stratégiai hatást teszi első helyre, és azután határozza meg a tennivalókat, amelyek valószínűleg elvezetnek a célhoz. Az áhított célról szőtt álom realiztikusabbá válik, ha Henry Kissingerrel együtt megvizsgálunk két dolgot: Mit akarunk feltétlenül elérni? Mit kell feltétlenül megakadályoznunk?^[7] Kritikánk szellemében még hozzátehetjük: És mit

adhat ehhez hozzá a technika? Egy hatásalapú megközelítés nem az okból, hanem abból a végállapotból indul ki, amibe Európának el kell jutnia.

Gyorsan világossá válik: hosszan sorjáznak azok a dolgok, amelyek ideális esetben nélkülözhetetlenek Európa számára. Egészen bizonyosan közéjük tartozik a dübörgő gazdaság és a piaci erő, a stabil valuta, a jólét és a szegénység visszaszorítása. Az európai belső és külső biztonság, valamint a béke. A társadalmi mobilitás és egység. Nincs helye köztük viszont a város és vidék közti szakadéknak, annál inkább a klímavédelemnek, a szabadságnak, a demokráciának, a jogállamiságnak és a minőségi médiának. Az európaiak közti barátság elmélyülésének. Megbízható szövetségeknek – dacára a függetlenségnek és autonómiának. Sokszínűségnek és nyitottságnak.

Európa még mindig nagy potenciállal rendelkezik. Ha akarná, még ahhoz is megvolna a képessége, hogy *soft power*t alkalmazó hegemoniális hatalommá váljék, nem az egész világ számára, hanem önálló, harmadik rendszeralternatívaként az amerikanizáció és a kínai álom között. Ekképpen vonzó volna mindazon nemzetek számára, amelyek a két alternatíva közül egyikért sem lelkesednek. Egy ilyen Európa – nemcsak saját érdekétől, hanem némi altruizmustól is vezetve – ki tudná vívni, hogy elfogadják a nemzetközi szintén: feltéve, hogy más demokratikus államokkal szorosan egyeztetett multilaterális politikát folytat, s eközben világosan megfogalmazott alapelvek alapján cselekszik.

Ha jelenleg egyre kisebb is a remény, hogy még hihetően megfogalmazható egy olyan európai identitás narratívája, amely – Kelet és Nyugat, Észak és Dél ellentéteinek dacára – a különbözőségben megvalósuló egységen alapul, Európa szívében még mindig vannak államok, amelyek képesek előidézni a változást és megerősíteni Európát, aktívan síkra szállni a demokráciáért, az emberi jogokért és a jogállamiságért: mindennekelőtt az eurohegemón Németország. Az ország Európa gazdasági motorja és legnagyobb nemzetgazdasága, az EU legnagyobb nettó befizetője, és nemrég még exportvilágbajnok is volt. Számos dobogó legmagasabb fokára jutott fel. Mivel Európa gazdasági sikere jelentős mértékben Németország vállán nyugszik, a sok mindenben sikeres országot nagy felelősség is terheli. A vezetés inkább kötelezettség mindig, semmint renomé és rang.

A múlttal ellentétben Európa eljövendő vezetői kompetenciája már nem kizárólag piaci erejéből táplálkozna, hanem kulturális vonzerejéből is, különösen – és a konkurens ázsiai rendszerrel ellentétben – abból az emberképből, amely szerint minden liberális-demokratikus társadalmi rend alapja a szuverén individuum. Ennek vonzerejét erőszakkal természetesen lehetetlen volna érvényre juttatni, hatékonyan kellene azonban biztosítani és védelmezni. Így Amerika relatív visszahúzódásából nemcsak Kína és Oroszország, hanem Európa relatív felemelkedése is lehetne. Csakhogy ehhez Európának egyértelműen kellene reagálnia Amerika visszavonulására, és előmozdítani azt, ami Donald Trump számára nem tűnik már fontosnak: a de-

mokráciát, a jogállamot, a szociális piacgazdaságot és mindene-előtt biztonságot a határain belül és kívül, a közvetlen szomszédságában. Európának egy erős demokrácia-utópiára lenne szüksége a jövőjére nézve.

A hegemoniális hatalom előfeltételei

Ennek elérése nem lesz könnyű, mert már régóta nincs minden európai kormány meggyőződve a demokratikus eszmény helytálló voltáról. A kételyt le kell győzni, a demokratikus meggyőződések pedig ismét begyakorolni. Az európai értékek megőrzése és még inkább az érvényesítése ugyanis azzal még nem következik be, hogy európaiak siránkozni kezdenek Kínában, Oroszországban és Amerikában: „Kérjük, hagyjatok fel a világ rendjének átalakításával!” Ha vádaskodunk, vitatkozunk, a továbbiakban is az tesszük, mint eddig, és a múlton révedezünk, a demokrácia nem marad fenn, nem érvényesül. Egy határozott demokráciapolitikának csak akkor van esélye arra, hogy hatásos legyen, ha minden diplomáciai, információtechnológiai, katonai és gazdasági eszközt kihasznál.

Mindazonáltal van a demokráciapolitikának egy rendszer-szintű fékje, amely magában a profitlogikában gyökerezik. Nevezetesen a gazdaságosságra törekvés, vagyis hogy az ilyen politika költségeit minél alacsonyabban tartsuk. Ez esetben a demokráciapolitika célja nemcsak a hatás, hanem a hatékonyság elérése is lenne. Minimális ráfordítással kellene működtetni, a lehető legcsekélyebb ráfordítással, a demokráciának a szomszé-

dos államokban való előmozdítása esetén pedig fegyveres erők és kiképzők lehetőleg minél ritkább bevetésével külföldön, illetve emberkereskedők elleni járőrhajóval a Földközi-tengeren.

A hatékonyság azonban nem mércéje egy vonzó világpolitikának. A hegemonia, mint a történelemből tudjuk, a *soft power*en alapul, azon a varázson, ami a meggyőződés erejéből ered. Tudjuk továbbá a múltból, hogy az ilyen hatalomhoz alapok kellenek. Csak úgy, magától nem jön létre – és drága lehet.

A demokráciapolitika vonzerejének legfontosabb előfeltétele eszerint nemzetközi közjavak, a *commons* – virágzó gazdaság, stabil valuta és tartós béke – rendelkezésre bocsátása, és pedig ellentételezés nélkül, de legalábbis csekély költségek fejében.^[8]

Az Európai Unió közjavai közé tartozik **a gazdasági stabilitás – világos szabályozási normákkal**. Különösen Európa peremövezeteire kellene kiterjednie, ahol még nem terjeszkedett el Kína, ugyanis a népköztársaság épp most nyújt készséggel hiteleket az európai perifériákon.

Miközben pedig az amerikai dollár lassan elveszti „biztos kötő” jellegét, ahová nyugtalan időkben a Washington vezető szerepében hívó befektetők elmenekülhetnek, az **euró** átvehetné a biztonságos globális referenciavaluta szerepét – legalább is elméletileg.^[9] Ehhez azonban az eurozónának először meg kellene oldania az euróstabilitásával kapcsolatos problémákat, különösen azt a jelenleg sürgetően fontos kérdést, hogy mi történjék a továbbiakban Olaszországgal.

Valakinek foglalkoznia kell a déli irányból érkező migrációs nyomással, ily módon pedig szükségképpen a klíma- és fejlesztés-

tési kérdésekkel is. Feltétlenül a közjavakhoz tartozik a **béke és biztonság** is, az európai demokráciapolitika esetében a *Pax Europaea*. Az Európai Uniónak kellő elszántságot és következetességet kellene tanúsítania, hogy maga gondoskodjon az 500 millió európai biztonságáról. A béke közjaváért való aggodalom nemcsak politikai jelleggel nyilvánulhat meg, megköveteli a védelmet és a katonai biztosítást is.

„Külpolitikát nem lehet haderő nélkül folytatni”, foglalja össze Wolfgang Ischinger sokéves diplomáciai pályájának tapasztalatait. „Másként a külpolitika írott malaszt marad.”^[10] Európának, teszi hozzá, több autonómiára van szüksége a védelemben és a stratégiában. Nemcsak a védelem területén kell azonban komoly kiadásokra számítani. Az Egyesült Államok annak érdekében, hogy uralja az új közjavakat, a világtengereket, a légteret, a világűrt és a „cyberspace-t”, dollár-ezermilliárdokat fektetett be, és mindig esélyt biztosított az innovációnak. Ha egy világrendszer meg akarja alapozni igényeit, elengedhetetlenek az **innovatív teljesítmények**. Az új technológiákat, a globális műholdas navigációt, az internetet és a virtuális javak sokaságát, amelyek mind a hálózatosításon alapultak, az Egyesült Államok ha nem is ingyen, de ellentételezés nélkül bocsátotta rendelkezésre. Különösen az európaiak profitáltak ebből. Annak azonban, hogy megkapták az Egyesült Államokból a digitalizáció eredményeit, az volt az ára, hogy ellenőrzés alá került a teljes adatforgalmuk, az NSA, az amerikai Nemzetbiztonsági Ügynökség hozzáférést kapott az internet csomópontjaihoz és po-

tenciális betekintést az európai gazdaság és ipar adataiba, amelyeket amerikai vezetésű számítóközpontokban tárolnak.

Az európai demokráciapolitikának azzal kellene kezdődnie, hogy az innovációkat és az új technológiákat politikai hatásuk szempontjából is megvizsgálják. Különösen a mesterséges intelligencia számít világszerte katonai kulcstechnológiának. Mindazonáltal éppen Németország az, aki azt kívánja, hogy a katonai felhasználású mesterséges intelligenciát minősítsék vissza a kutatás és gazdaság pusztá melléktermékévé.^[11] Ezt a mesterséges intelligencia superhatalmai egészen másként látják. Innovációikban kettős, katonai és civil felhasználhatóságra, *dual use*-ra törekszenek. Németország szemszöge ezzel szemben még mindig csak a versenyképességre és a profit logikájára szűkül le.

Európa békéjét és biztonságát szolgáló technológia

Bemutattuk a modern államközi konfliktusok sajátosságait: hogy egyre gyakoribbak az államilag vezényelt, háborúküszöb alatti támadások, köztük a digitális kémkedés és szabotázs. Az online felforgatás aláássa a demokratikus kormányok iránti bizalmat: eszközeit alternatív tényeknek, *social engineering*nek vagy *doxing*nek nevezik. Miközben pedig világszerte vita folyik a fegyverek autonómiájáról, a támadó autonóm gépek – amilyeneket, fontos prioritásként kezelve őket, Oroszország, Kína, valamint az Egyesült Államok kutató és fejleszt – fognak egyre na-

gyobb kihívást jelenteni Európa számára. A digitalizáció megváltoztatja a hadviselést, a 20. századból származó veszélyekhez alapvetően új fenyegetéseket társít, és új csatateret hoz létre.^[12]

Vajon alkalmasak-e arra az új technológiák, hogy támogassák a demokráciapolitikát, és biztonságot teremtsenek? A védelem, az elrettentés és az eszkaláció éppúgy hozzátartozik a *Pax Europaea* biztosításához, mint a polgárok és a digitális infrastruktúrák fokozott tűrőképessége. Aki az európai modellt, valamint partnereit és szövetségeseit meg akarja védeni a külső kényszertől vagy agresszív cselekményektől, annak választ kell találnia az új csatater kihívásaira. Páncélosokkal ugyanis nem lehet legyőzni a digitális harcosokat. Azzal kapcsolatban, hogy miként festhetne egy ilyen válasz, hadd vázoljak fel néhány elképzelést. Fantáziát igényel – miközben meg is mozgatja azt –, emellett sok kiegészítést is.

Nagyobb biztonság teremtése a környezeti intelligencia számára

Az európai államok és vállalataik ugyan állandóan tökéletesítik a digitális támadások elleni védekezést, de már e szurkálások száma is elképesztően nagy. És egyre kifinomultabbak lesznek. Egyre gyakrabban irányulnak szállítóláncok, a pénzügyi rendszer vagy számítóközpont-üzemeltetők ellen. Már pontszerű támadási sikerek elegendők ahhoz, hogy bizalmatlanságot ébresszenek a hálózatiság biztonságossága iránt, mert például

már nem működik megbízhatóan a mindennapi használati cikkekkel való ellátás, esetleg nehezebb benzinhoz jutni, vagy mert a szupermarketek polcairól eltűnnek a mezőgazdasági termékek.

Egyelőre még ott tartunk, hogy a környezeti biztonság kérdéseit illetően magukra hagyják a vállalatokat és a szolgáltatókat. Valójában a legtöbbjük már régen nem képes gondoskodni környezeti intelligenciája biztonságáról – legalábbis ha nem éri el a konszernnagyságot. Így például a kisebb kórházak még saját digitális biztonságukról is alig tudnak gondoskodni. Ennek költségei ugyanis magasak, nem terhelhetők rá a betegátlányra. Így a digitális támadások – mint amilyen 2018. november 8-án a bajor Fürstenfeldbruck klinikája elleni volt – ahhoz vezethetnek, hogy a mentőjárművek nem tudnak kivonulni, és még életveszélyben lévő betegek felvételére sincsen lehetőség. A fürstenfeldbrucki klinika elleni támadás esetében az mentette meg a súlyos betegeket, hogy a környékbeli kórházak nem voltak hálózatra kapcsolva a megtámadott intézménnyel, így át tudták hidalni a kiesését. Az infrastrukturális biztonság tehát a decentralizáción is múlik – és a legkevésbé sem azon, hogy minden mindezzel összekötve hálózati kapcsolatban legyen az *internet of everything* révén.

Egy hegemoniális hatalomnak meg kell őriznie lakossága, partnerei és szövetségesei digitális infrastruktúrába vetett bizalmát. Ha egy vezető nemzet képes szavatolni a környezeti intelligencia biztonságát, és kontrollálni tudja az ellene irányuló károkozást, nemcsak hatalmi monopóliumát erősíti, hanem pol-

gárai is biztonságban érezhetik magukat. A támadásoktól való félelem relativizálódik, a bizalom nő.

Ha Európa bebizonyítja, hogy eleget tud tenni a 21. század biztonsági kihívásainak, az EU-pesszimizmus is csökkenni fog. Ahelyett, hogy magára hagyná a lakosságot a digitális biztonsági kérdésekben, Európa dönthetne úgy, hogy világelső lesz a környezeti intelligencia nagyobb biztonságáért folytatott küzdelemben. Ez konkrétan annyit jelent, hogy az állam nemcsak az állami létesítmények elleni hibrid támadásokat védi ki, hanem együttműködést alakít ki a magánszférával, ahogyan ezt Ausztriában már 1975 óta a Biztonságos Ausztria Kuratórium (KSÖ) teszi. Előmozdítja a számítástechnikában tehetséges emberek képességfejlesztésébe és a biztonságos hétköznapi használati tárgyakba történő beruházásokat. A programozásban tehetséges gyerekek ugyanis nem szükségképpen jó tanulók, az „okos” tárgyak pedig nem minden körülmények közt biztonságosak. A tehetségeket fel kell fedezni és támogatni – a tárgyakat pedig tökéletesíteni.

Éppen Németországnak volna számos lehetősége, hogy jóval nagyobb biztonságot teremtsen a környezeti intelligenciában. Ami a precíziós mérőberendezések és szenzorok előállítását illeti – márpedig ezek alkotják a környezeti intelligencia legfontosabb részét –, jó hírű nemzet a német. Szabványokat kell megállapítani. A modern szenzoroknak tudniuk kell titkosított kommunikációt folytatniuk kontrollcentrumaikkal, hogy ezáltal minimalizálódjék a *spoofing* miatti hamis információk továbbításának veszélye. A kódolás még inkább jövőbe mutató. Miközben

a kutatás lázasan keresi a kvantumszámítógép gazdaságos üzemű alkalmazásának koncepcióját, az már ma is bizonyos, hogy gyorsan és hatékonyan dekódol. A kvantumkomputerek az összes mai titkosítást – amely számok prímtényezős felbontásán alapul – egytől-egyig könnyűszerrel feltörik majd. A holnapi biztonság érdekében elengedhetetlen lenne kutatásokat folytatni a jövőbeli titkosítási technológiák területén.

A védelem kiépítése

Ami a környezeti intelligenciát érő támadások elleni, német haderő által nyújtott védelmet illeti, ma egyaránt vannak jó és rossz híreink.

A német fegyveres erők éppenséggel jól fel vannak készülve digitális támadók elhárítására. Nem szenvednek hiányt sem tartalékokban, sem know how-ban, sem pénzben. Ez a jó hír. A rossz hír az, hogy digitális támadások ellen csak saját hálózataikat védik, az egyre nagyobb civil környezeti intelligenciát azonban nem. A harci forгатókönyvek magukban foglalják az ellen-séges katonai kapacitások zavarását, a saját csapatok támogatását az új csatatéren, továbbá a felderítést – de csak ezekre szorítkoznak. A gazdaság és az ipar elleni támadások kivédése mindeközben hatalmas kultúrsokkot okozna a haderő számára: talán a frankfurti Amazon számítóközpont elleni digitális támadásokat kellene elhárítaniuk, ily módon ellátva belföldi katonai feladatokat? (A létesítmény, lévén az internet gerince, mára rendszerrelevánsabb infrastruktúra, mint a két német nagy-

bank.) Mindenesetre a digitális támadások kivédését olyan civil hatóságokra hagyják Németországban, mint a titkosszolgálatok. A *hacking back* a Szövetségi Hírszerzőszolgálat, és nem a haderő hatáskörébe tartozik. Lehetséges azonban, hogy a 21. században az új hadszíntér gyors fejlődésével a honvédelem definíciója ugyanúgy túlhaladottá vált, mint számos más (civil) koncepció is.

Mindazonáltal a környezeti intelligenciát érhetik olyan támadások, amelyek nyomán védelmi eset állhat elő: ezek azonos megítélés alá esnének az ENSZ Alapokmány 51. cikkelyében szereplő fegyveres támadásokkal. Egy okos democráciapolitika a szövetségesekkel és partnerekkel multilaterális egyezményekben határozná meg, mely támadások idéznének elő védelmi esetet, illetve léptetnének életbe segítségnyújtási kötelezettséget: digitális szabotázs nukleáris reaktorok vagy az alapvető egészségügyi ellátás ellen, beavatkozások a légiközlekedés biztonságába azzal a következménnyel, hogy polgári légi járművek zuhannak le – vagy szabotázs a pénzügyi rendszer ellen. Annak, aki a digitális választásokhoz hasonló demokratikus intézmények elleni szabotázst nem akarja felvenni a védelmieset-katalógusba, legalábbis képesnek kell lennie a támadások felderítésére, következésképpen pedig büntetőjogi üldözésére. Erre szolgál például Robert Mueller amerikai különleges ügyész tevékenysége.

Az átfogó democráciapolitika szellemében fontolóra vehetők a proaktív védelmi magatartás gondosan végrehajtott megelőző intézkedései is. Ezek offenzív jellegűek, és megzavarják az el-

lenfél támadásait, mielőtt kár keletkezne a megtámadott saját környezeti intelligenciájában. A hekkereket meg lehet gátolni abban, hogy hozzáférjenek szervereikhez, de az adatok is elláthatók olyan lokációs rendszerrel, amely adatlopás esetén megkönnyíti a megtalálásukat, és a támadó azonosítását. Itt ismét felvetődik az illetékesség kérdése. Minden állam szabadon dönthet arról, hogy haderőit, nemzeti gárdáját, paramilitáris csoportjait, különleges rendőri erőit vagy titkosszolgálatait bízze-e meg a feladattal. Nem az a fontos, hogy az állam hogyan nevezi, illetve szervezi védelmi erőit, hanem hogy milyen feladatokat látnak el.^[13]

A határozott demokráciapolitikának azonban előzőleg választ kell adnia egy kérdésre, arra tudniillik, hogy egyáltalán mennyiben tesz lehetővé a nemzetközi jog egy megelőző csapást. Az Obama-adminisztráció egyik kormánytanácsadója már évekkel ezelőtt megállapította: „Nincs még egy olyan probléma, amelyre a kormány jogászai több időt áldoztak volna ily csekély haszonnal, mint arra a kérdésre, hogy hogyan alkalmazandó a nemzetközi jog a digitális támadásokra.”^[14]

A demokráciapolitikától azonban feltétlenül el kell várni, hogy mindig a jogot részesítse előnyben. Akkor pedig szükségképpen nem engedhető meg minden offenzív intézkedés. Ez annyit jelent, hogy a demokráciapolitika világítótornya és vezércsillaga lesz egy olyan koherens stratégiának, amely meghatározza, mely intézkedések valóban megengedettek digitális támadások ellen, és melyek nem. Itt is érvényes, hogy szükséges a partnerekkel való multilaterális egyeztetés.

A megelőző védelem még egy további következménnyel jár. A hegemoniális hatalomnak minden helyzetre fel kell készülnie. Készen kell állnia, és el kell képzelnie az elképzelhetetlent – azt, hogy egy konfliktus eszkalálódik, és erőszakos katonai összeüt-közéssé fajul.

„Nem félnek tőlünk”: elrettentés és eszkaláció

Vajon egy demokráciapolitikát folytató állam képes-e gondoskodni a környezeti intelligencia biztonságáról, ha digitális tekintetben kellően felkészül, hogy ezzel elrettentse hibrid támadást tervező ellenfeleit? A kérdés végső soron nem egyébre irányul, mint a megsemmisítő második csapás végrehajtásának képességére. Ilyenformán az ellenfél félelmére alapozva kerül sor olyan offenzív digitális képességek és technikák kifejlesztésére, amelyek révén titkosított rendszerekbe lehet behatolni, vagy digitális támadások elleni védelem céljából valós időben saját kártékony szoftvert bevetni. Az elrettentés mindig kommunikálja a támadás szándékát is, ennek demonstrálása a politikai eszköze.

A kommunikáció és a demonstráció eleve két olyan kulcsszó, amely az elrettentéssel összefüggésben tesz szert a legnagyobb jelentőségre. Bizonyosan nem vonja kétségbe senki, hogy (egyelőre még) az egész világon az Egyesült Államok rendelkezik a legjobb digitális képességekkel. Erről azonban magának az USA-nak csak homályos fogalmai vannak. Tudja, hogy technológiai előnyét már csaknem elveszítette a nyakába lihegő Kínával

szemben – ehhez azonban még hozzá kell szoknia.^[15] Amerika ugyan még sok mindent tehet környezeti intelligenciájának biztonságáért, ami azonban ennek a teljesítménynek a tényleges dimenzióit illeti, senki sem tud mondani biztosat. Az amerikaiak nem akarják, hogy belelássanak a kártyáikba. Az, hogy más országok ellen milyen digitális hírszerzési és szabotázstevékenységet folytatnak, és hogyan játsszák ki őket, továbbra is titok, zárt ajtók mögötti, titkosszolgálati ügy. Oroszországot ez nem rettent el, és látványos hibrid támadásokat intéz Amerika ellen, ahogyan ez a 2016-os elnökválasztási küzdelem során is történt.

Az elrettentés a hidegháború idejéből származó koncepció, és úgy tűnik, mintha kívánt hatása csak az atomfegyverekkel és ezek rettenetes, aránytalanul nagy megsemmisítő potenciáljával összefüggésben jelentkezne. Eszerint az elrettentés nem adaptálható minden további nélkül a 21. század hibrid támadásaira – vagy csak akkor, ha egy állam arra az esetre, ha egy ellenfele súlyos hibrid támadást hajtana végre ellene, nukleáris válaszcsapást helyezne kilátásba. Az Egyesült Államok tulajdonképpen elkötelezte magát amellett, hogy pusztító digitális támadásokkal szemben harcászati atomfegyvereket vet be; ezt sejteti az amerikai külpolitika Donald Trump alatt végbement drámai eltolódása, amelyet a nukleáris fegyverek alkalmazásával kapcsolatos, 2018 februári állásfoglalás valószínűsít.^[16]

Ennek ellenére van egy történelmi példa a sikeres digitális elrettentésre. Éppen Barack Obama amerikai elnök volt az, aki habozott erőteljes választ adni a 2016-os amerikai választások-

ba való orosz beavatkozásokra. Obama meghekkeltethette volna az oroszok szervereit, kártékony szoftvereket telepíttethetett volna rájuk. Megszakíttathatta volna az összes támadó szerver áramellátását. Kiterjeszthette volna az Oroszország elleni szankciókat, zároltathatta volna orosz állampolgárok bank-számláit.

Csak hogy semmi ilyesmi nem történt. A félelem, hogy Oroszország még jobban kiélezheti a helyzetet, erősebb volt az akaratnál, hogy védekezzenek a választásokba történő orosz beavatkozás ellen. Az eskalációs spirál alakulása során ugyanis mindig felvetődik a kérdés, hogy vajon miként reagál az ellenfél egy-egy védelmi intézkedésre. Netán rendszerének külföldön élő kritikusait mérgezi meg? Esetleg diplomatákat utasít ki? Kémtevékenység vádjával lefogatja a megtámadott országnak a saját területén élő állampolgárait? Egy gombnyomással alvó kártékony programokat aktivál az áldozat-állam infrastruktúrájában?

Az elnök alighanem ennyire sem ment megfontolásaiban. Barack Obamát már az a félelem is visszatartotta az amerikai választók riadóztatásától, hogy az amerikai lakosság egy – mégoly gondosan kidolgozott – védelmi intézkedést is az Obama-adminisztrációnak a 2016-os választási küzdelembe való beavatkozásaként értelmezhet. Oroszországnak ismét csak nem kellett tartania attól, hogy meg kell fizetnie hibrid támadásának árát.

Ha az elrettentés nem ér el kellő hatást, okosabb teljesen lemondani róla, és a saját erőket jobb elhárító intézkedésekre és az esetleges zavarok elleni nagyobb védelemre összpontosítani.

Ennek érdekében még a német kormánynak is le kell mondania valamiről: az offenzív intézkedésekről. Annak tehát, aki Németországhoz hasonlóan offenzív technológiákat kutat, s olyan különleges ügynökséget hoz létre mint a Biztonsági Szféra Informatótechnikai Központja (Zentrale Stelle für Informationstechnik im Sicherheitsbereich, ZITiS), amely rejtjelfejtéssel foglalkozik és megfigyelési technológiákon dolgozik, tisztában kell lennie azzal, hogy eszközei offenzív, nem pedig defenzív jellegűek. Egy hegemoniális hatalomnak azonban, amely részben offenzív módon szándékszik biztonságot teremteni, számolnia kell a következményekkel is, és készen kell állnia, hogy elviselje az eskalációt és az ellentámadásokat. Ha más államok hasonló módon felfegyverkeznek digitálisan, előfordulhat, hogy az eskalációs spirál végén mégis csak a fizikai erőszak és a kinetikus hatású fegyverek állnak, amikor a digitális elrettentés már elveszíti fenyegetéspotenciálját.

Annak, aki mégis ragaszkodik az elrettentéshez, nyíltan kell kommunikálnia. A 2018-as amerikai időközi választások előtt az Egyesült Államok ismét a demokráciájába történő orosz beavatkozást azonosított, amiről utóbb nyíltan értesítette a támadókat. [17] A „mérlegelési esély megadását szolgáló titoktartás” új koncepcióját alkalmazva az USA egészen másként reagált, mint 2016-ban, amikor Washington az oroszok szóbeli cáfolatára semmilyen kommunikációs lépést nem tett. A nyílt értesítések elküldésével az Egyesült Államok ezúttal világossá tette, hogy a támadásokat egészen az egyes hekkerekig képes átlátni.

Ezúttal erőt vett gőgjén, és felhagyott a titkolózással. Ha most ráadásul még következetesen, büntetőjogilag is eljár a támadók ellen, jók az esélyei, hogy a jövőben védettebb lesz. Az amerikaiak mindenesetre így gondolkodnak.

Kíváncsi lenne egy stratégiai kódex, amely – ellentétben a Tallinni kézikönyvvel – kötelező elhárítási, elrettentési és eszkalációs magatartási normákat fogalmaz meg. Egy ilyen stratégiai kódex multilaterális egyeztetés eredményeként kellene, hogy létrejöjjön. Magántulajdonban lévő technológiai óriásokat is be kellene vonni az egyeztetésbe, nemcsak támogatásuk biztosítása céljából, hanem azért is, hogy szorosabb jogi kötelékek vonatkozzanak rájuk.

„Ha az a helyzet – állapítja meg Wolfgang Ischinger nyugalmazott nagykövet –, hogy egész sor cégünk van, amely tízszer, százszor, ezerszer, tízezerszer akkora gazdasági erővel rendelkezik, mint a legtöbb állam – és még nő is a számuk –, vajon mikor jön el az a pont, amikor ki kell mondanunk: ezeknek a cégeknek voltaképpen egy testületben is képviseltetniük kell magukat? Őket is be kell vonnunk. Vajon alávéthetjük-e őket azoknak a szabályoknak, amelyeket államoknak is tiszteletben kell tartaniuk?”^[18]

A Microsoft javasolt egy Digitális Genfi Egyezményt, a Deutsche Telekom AG vezérigazgatója, Timotheus Höttges egy Biztonsági Világszervezetet, amely az Egészségügyi Világszervezettel volna összehasonlítható.^[19] Mindig is lehetséges opció lesz a már meglévő nemzetközi jog értelmezése, adott esetben kiterjesztése, vagy a vállalatok kötelezettségvállalása, a *corporate so-*

cial responsibility, a vállalatirányítás kontinuitásának keretei közt, aminek megsértéséért a cégeknek és menedzsereiknek szükség esetén bíróságok előtt kell felelniük.

Bármiképpen jön is létre egy nemzetközi szabályzórendszer – az idő sürget. Amíg nem egyezünk meg normákban, egyszersmind határokbán is, a digitális támadások egyre veszélyesebbé válhatnak. Mivel a cégek – különösen a pénzügyi szférában – határokon átnyúlva mind gyakrabban folyamodnak digitális megtorló intézkedésekhez, az elrettentés és az eszkaláció nemzetközi kihívássá lett. Ám nemcsak az államoknak, hanem a technológiai vállalkozásoknak is felelősségteljesen kell viselkedniük, annál is inkább, mert nem feltétlenül tudják felmérni tetteik jogi és diplomáciai következményeit. Ennek ellenére a cégek egyre offenzívebben járnak el. Az offenzív válaszcsapáshoz nemcsak indítékkal, hanem eszközökkel is rendelkeznek. Ezért az offenzív intézkedések nemzetközi piaca sajnos bővülőben van – mégpedig teljesen szabályozatlan módon.

A magatartási normákkal és érvényesítésükkel kapcsolatos viták során olyan javaslatok születtek, amelyek kifejezetten biztosító intézetek bevonását irányozzák elő. A digitális védekezés során adódó kockázatokat nekik kellene átvállalniuk, illetve nekik kellene megfogalmazniuk, hogy konkrétan milyen károkért és kockázatokért állnának jól. Ez bizonyos digitális intézkedések nyomán keletkezett károkat kizár.

„Ha az államok, álláspontjukban teljesen bizonyosan, azt mondanák: »Ez a mi számunkra támadás«, és: »Ez a mi számunkra nem támadás«, vagy: »Így és így reagálunk, ha...«, ak-

kor minden meglehetősen világos volna (...)”, mondja Tobias Vestner svájci nemzetközi jogász. Egyes akciókat akkor nem is engedélyeznének, köztük az ipari kémkedést sem. Tilos volna például a termelő vagy gyógyszeripari vállalatok elleni támadás is. A tisztán védelmi intézkedések megengedettek lennének, kockázatos offenzív eszközöket ellenben csak végső megoldásként lehetne bevetni – és alkalmazójuknak igazolnia kellene, hogy minden feltétel adva van egy jogos válaszcsapáshoz, és hogy minden elővigyázatossági és biztonsági intézkedést megtett a kockázatos akciók valóban felelősségteljes végrehajtása érdekében. Arról, hogy a vállalatok tartsák magukat a meghozott szabályokhoz, egy mindig működő irányító mechanizmus gondoskodna: a biztosítási díj mértéke, azaz a pénz. „Ezt azonban – zárja fejtegetését Tobias Vestner – nem akarják.”^[20]

A védelmi intézkedések azonban megmaradnak legfőbb parancsnak, még akkor is, ha soha nem lehet maradéktalanul kizárni, hogy támadások hibákat idézzenek elő. Egy vigaszunk ezért lehet: az infrastrukturális tűrőképesség nagyobb biztonságról gondoskodhat egy ellenséges támadás esetén.

Tűrőképesség teremtése osztott infrastruktúrákkal

A központosított struktúrák, mint például azok a rendszerarchitektúrák, amelyek úgynevezett *hub-and-spoke* (kerékagy és küllő) megközelítést alkalmaznak – amelyekben sok végpont

egy központi csomóponton keresztül kommunikál – összeomlanak, ha a központ kiesik.

A mai környezeti intelligencia, a dolgok internetje, centralisztikus elv szerint működik, azaz a környezeti intelligenciából származó adatokat központi helyen, leginkább amerikai technológiai óriások számítóközpontjaiban tárolja. Ezekből további feldolgozás után impulzusként ismét a helyi berendezésekbe küldik vissza. Ha egy támadónak sikerülne egy ilyen centrális csomópontba behatolnia, vagy végzetes csapást mérnie egy rendszerreleváns számítóközpontra, a rendszer egésze kerülne veszélybe, mert a centralisztikusan vezérelt digitális infrastruktúrák nagy kiterjedésű részei iktatódnának ki.

Ehhez képest a decentrális infrastruktúrák robusztusabbak, ezekben a hibatűrés elve érvényesül. Egy kritikus infrastruktúra elleni támadás esetén ugyan számításba kellene venni a rendszer egy részének kiesését, azonban az egészet mint ilyen, legalább részben, tovább lehetne működtetni.

Egy ilyen *system of systems*ben (rendszerekből álló rendszer) az adatokat nem egy centrális csomóponton át közlik, hanem helyben dolgozzák fel, ahol is minden alrendszer saját helyi intelligenciával rendelkezik. Igaz ugyan, hogy ez az *edge computing* (periférikus adatfeldolgozás) kénytelen megküzdeni a maga egészen sajátos kihívásaival – van helyben elégséges processzorteljesítmény? Biztosítva van az áramellátás? –, de sikeresebben védheti a magánszférát és a sáv szélességet, mert a nyersadatokat nem szünet nélkül küldi a felhőbe. A központi számítóközpontokhoz küldött alkalmankénti – például a szolgálta-

tások árverezésére vonatkozó – szolgáltatási igények így már csak a helyi tevékenység minőségének javítását szolgálják.

Ténylegesen csak az autonóm, ami önállóan is tökéletesen működik, anélkül, hogy egy számítógépes felhőtől függene. Igazi autonómia esetén a kommunikáció csak opcionális akció, bizonyosan nem kényszer. Erre 2018 őszén egy berlini konferencián igen találó módon maga Wenshuan Dang, a Huawei Technologies vezető stratégiafejlesztője mutatott rá. Aki az autonóm autózást úgy valósítja meg, hogy az önirányító autók csak 5G-technológia és egy központi számítógépes felhő segítségével működnek, szerinte nem értette meg az autonómia koncepcióját.^[21]

A jószándékú laikus most azt gondolja, a nagyobb tűrőképesség érdekében a rendszereket észszerű decentralizálni és felosztani. A *system of systems* azonban nem a szabályt, hanem a kivételt jelenti. Annak, hogy az infrastruktúrák centralizmusra épülnek, legalább két oka van.

Először is, az osztottság a hatékonyság rovására megy. Ismét csak az üzemgazdasági szemlélet érvényesül, ugyanis az osztott rendszereket kényelmetlenebb kezelni, és gyakran nehezebb karbantartani. Folyamatos üzem mellett a disztribúció gyakran több pénzbe kerül, és eleve nem világos, milyen bevételek ellentételezik a nagyobb robusztusság és biztonságosság költségeit.

Másodszor, a koncentráció azoknak a neoliberais igényeknek az egyike, amelyekhez az amerikai technológiai óriások már csak neoliberális rendszerben való szocializációjuk miatt is ragaszkodnak. Amazon, Google, Facebook: mindegyik hatalmas számítóközpontokat épített fel, amelyeket, a tudományos számí-

tások centrumaiként – magyarán az agyonreklámozott gépi tanulás és a mesterséges neurális hálózatok központjaiként –, szeretnének kihasználva látni. Ezúttal is a monopólium, vagy legalábbis az oligopólium hatalmi pozíciójáról van szó. A technológiát centralizálni akaró oligopolisták egyáltalán nem lehetnek érdekeltek az osztott struktúrák alkalmazásában. Ellene mond az ideológiájuknak. A neoliberalizmusból és a célul kitűzött versenyképességből ugyanis csak az profitál, aki maga áll annak a versenynek az élén, amely „a mások gazdasági rendszerének ellenőrzéséért folyik anélkül, hogy vállalni kellene a következményeket”^[22].

A társadalom beoltása a támadások ellen

2017 választási szuperév volt Európa számára, Németország, Franciaország, Nagy-Britannia, Hollandia és Ausztria egyaránt a szavazóurnákhoz szólította választópolgárait. És mind riadtan találgatták: vajon Európában is megismétlődik, ami egy évvel korábban az Egyesült Államokban történt? Vajon beleavatkozik Oroszország az európaiak demokratikus választási folyamataiba? Az európaiak lázas munkával és az idő szorítása miatt olykor rögtönözve igyekeztek gondoskodni nemzeti demokratikus választásaik biztonságosságáról.

Ma már ismerjük az eredményt: nem sokon múlt, de baj nélkül megúsztuk. Persze valamelyest minden országban máshogy alakultak a dolgok. Németországot gyakorlatilag megkímélték a

támadások. Ami nem feltétlenül jó, mert a választók a jövőben félvállról vehetik a veszélyt, hogy bizonyos államok kívülről megpróbálják erőszakosan megváltoztatni egy jelölt vagy egy párt választóinak preferenciáit, magát a tulajdonképpeni választási folyamatot, sőt esetleg a választásokon való részvétel arányát is. Oroszország visszafogta magát, ami máig találgatásokra ad okot. Lehet, hogy elrettentő hatást fejtettek ki a figyelmeztetések, amelyeket Németország Moszkvához intézett: aki hekkerkedik, piros lapra számíthat. Donald Trump kiszámíthatatlan viselkedése talán arra indította a Kremlt, hogy újraértékelje Európához fűződő kapcsolatait. Végül is jó hasznát lehet venni olyan partnereknek, akik Moszkvával közösen keresnek kompromisszumokat válságrégiókban.

Emmanuel Macronnak kevesebb szerencséje volt, talán azért is, mert őt nagyon megközelítette populista ellenfele, Marine Le Pen, a Kreml szövetségese. Választási kampánya mindenestre jól elő volt készítve, és meglepően kreatívrá sikeredett: a *La République en Marche* (A köztársaság lendületben) kellőképpen felfegyverkezett az orosz hekkerek elleni küzdelemre. Emmanuel Macron mozgalmának IT-specialistái a phishing-weboldalakat olyan jelszavakkal árasztották el, amelyek közül sok valódi, ugyanakkor sok hamis is akadt. Ezzel a támadók nem számoltak, és alaposan lefoglalta őket a különbségtétel. A *La République en Marche* ezenkívül álcélokat is létesített digitális támadások kiprovokálására, amelyeket IT-zsargonban „mézesbödönöknek”, *honeypot*oknak neveznek. Macron mozgalma de facto hamis identitásokkal vágott vissza. A hekkereket kita-

lált franciák e-mail-postaládáiba irányították tovább, amelyeket előzőleg hamis információkkal spékelték meg. Ha a vélelmezett biztonsági réseket és az ezzel összefüggő állítólagos dezinformációt publikálták a közösségi médiában, Macron teamje villámgyorsan közölhette: ezek hazugságok, mi magunk gyártottuk őket, hogy a támadókat megtévesszük. Íme a bizonyíték...

Macron kampánya után voltaképpen senki sem mondhatta többé, hogy ami az informatikát illeti, az európaiakat a fejükre ejtették. A franciák ugyanis Barack Obamával ellentétben azonnal reagáltak: Franciaország népét jó és átlátható kommunikációval előre figyelmeztették.

Egyébként két államban, Franciaországban és Németországban analóg módon zajlik a választói szavazatok leadása, és az összeszámlálása is. Nem lehet számítógépen szavazni (kivéve a külföldön élő franciákat), és a szavazatokat sem géppel számlálják össze. A kézi számlálás mellett döntött Hollandia is. Csak a választási eredmények továbbításához használnak számítógépet, és ez lehet veszélyek forrása. Egy nemzet, amely kritikus infrastruktúrává nyilvánítja választási infrastruktúráját, e téren valószínűleg különleges biztonsági intézkedésekhez folyamodik.

Az Obama-adminisztráció már a 2016-os választási kampány idején arra jutott, hogy „beoltja” a választókat dezinformáció ellen. A legújabb kutatások eredményei azt igazolják, hogy a beoltottak képessé válnak a dezinformáció felismerésére, és arra, hogy lazán reagáljanak rá. Magára az immunizációra különféle módokon kerülhet sor, azonban mindig oktatáspolitikai intézke-

désről van szó. Már a diákokat is fel lehet világosítani az információs térben zajló felforgató, manipulatív tevékenységekkel kapcsolatban. Felnőttek számára egy európai kutatócsoport fejlesztett ki egy játékot, a *Bad Newst*.^[23] A cél a játékosok meg-edzése az információs tér olyan szereplőivel szemben, akik provokálnak, túloznak és sértegetnek – vagyis a trollok ellen. E célból maga a játékos bújik trollbőrbe, csal, hazudik és sérteget. A játék célja a troll-posztok gyors felismerésének megtanulása.

Mivel ezzel nem minden választót lehet elérni, a legfőbb követelmény továbbra is az, hogy a kormányok, pártok és a médiák is – az online platformokat sem kivéve – együttműködjenek, hogy megnehezítsék a demokrácia elleni felforgató támadásokat. „Technokogníció” az új varázsszó, amellyel kapcsolatban algoritmusok is szerephez jutnak. Feladatuk, hogy a digitális platformokon felismerjék és megjelöljék az álhíreket mint ilyeneket, illetve töröljék a hamis identitásokat. Időközben ez is gyakorlattá vált.

A technikai mechanizmusok mellett emberi kurátorok is központi szerepet játszanak. Még Donald Trump – ellenségeinek címzett – fenyegető tweetjei is ütköztek a platform felhasználási feltételeivel, és így büntetőjogi kategóriába esnek – nehezményezik a bírálói. Törölni kell őket. Jack Dorsey, a Twitter Inc. vezérigazgatója ezt az intelmet fogalmazta meg: még egy amerikai elnököt sem óv meg semmi a tweetelésből való kizárástól.^[24]

Meg kell még említenünk a valósággal szembeni legnagyobb kihívást, a *deep fake*st. Videók és hangfelvételek „mélyhamisítványai” valódi emberek képét-hangját produkálják, amint

olyasmiket tesznek vagy mondanak, amiket valójában sohasem tettek vagy mondtak. A mélyhamisítványok különösen azért alattomosak, mert hajlunk arra, hogy elhiggyük, amit a saját szemünkkel látunk. Ezért jelentenek nemzetbiztonsági problémát: könnyen idézhetnek elő politikai konfliktust, erőszakot vagy diplomáciai bonyodalmakat, embereket rágalmazhatnak meg, hamis bizonyítékként szolgálhatnak. A bökkenő az, hogy minél inkább tudatában vagyunk a videók és hangfelvételek hamisíthatóságának, annál kevésbé érint meg bennünket az autentikus képek üzenete.

A mélyhamisítványokat generatív ellenséges hálózatokkal (*generative adversarial networks*, GANs) hozzák létre, tehát szó szoros értelmében mesterséges intelligencia alkalmazásával. Két mesterséges neurális hálózat vetélkedik egymással. Mondjuk, hogy az egyik neurális hálózat, a generátor, létrehozza egy politikus képét. Egy másik neurális hálózat, a diszkriminátor, értékeli, hogy ez a kép mennyire különbözik a valóságtól. A generátor feladata olyan képek megalkotása, amelyeket a diszkriminátor már nem képes megkülönböztetni a valóságtól. Némi tanításra-tanulásra fordított idő elteltével létrejön egy szintetikus „valóság”, aminek a ténylegeshez a legcsekélyebb köze sincsen. Ezt azonban a néző vagy a hallgató, aki éppoly kevésbé képes különbséget tenni igazság és hazugság között, mint a diszkriminátor, nem tudja megkülönböztetni.

A mélyhamisítványok kivédésében az Európai Unió halad a leggyorsabban, és mint egy technológiai versenyben, finanszírozza az információtechnológiai felderítést, amelynek célja az

egyre tökéletesebb algoritmusokkal készülő *deep fake*-ek felismerése.^[25] Az USA-ban fontolgatják, hogy a videókat és hangfelvételeket „vízjelekkel” látják el, és a digitális platformokra való feltöltéskor szűrésnek vetik őket alá, hogy szavatolhassák az eredetiségüket. Mi több, Amerikára egyáltalán nem jellemző módon mérlegelik a regulációs beavatkozást, és a mélyhamisító algoritmusok alkalmazásának korlátozását – ritka eljárás volna ez az Egyesült Államokban, mert az ország mindenkor a libertárius, deregulált piacok mellett áll ki.^[26] Digitális időkben a nemzetbiztonság érdekében az eddig szokásosnál nyilvánvalóan messzebbre kell menni.

Ha egy demokratikus társadalomba egyszer beszivárog a dezinformáció, marad még a technikai lehetőség a nyugtalan-ság fokának mérésére. Ha a szociális kötelékek meglazulnak, és zavarok állnak be a rendben, nő a társadalmi káosz valószínűsége. Információteoretikusok „szociális entrópiáról” beszélnek. Amennyiben ez fokozódik, nő a veszély, hogy a társadalom egy új állapotot vesz fel, egy demokrácia például átbillenhet autokráciába. Ha ellenben a szociális entrópia csekély, a társadalom stabilnak számít.

A szociális entrópia mérésére lehetne tömegadatokat (*Big Datát*) alkalmazni, és kiszámítani egy indikátorértéket. Itt tág tere nyílik a koncepcionális gondolkodásnak: vajon a közérzet ilyen indikátor? Hát a társadalom gyűlölettől való átitatottsága? Az emberek államuk iránti bizalma? S ha igen, vajon mérni kellene ehhez a kormányuk korrupció iránti fogékonyságát? Min-

denesetre minél nagyobb a lakosság bizalma, annál érzéketlenebbek az állampolgárok a digitális felforgatásra.

A vonzerő alapja: az innováció

Aki vonzó akar lenni, annak innovációt kell felmutatnia. Nemcsak technológiai újítások tartoznak ide – lehetnek ezek bürokratikus, jogi vagy gazdasági természetűek is.^[27]

A digitális innovációhoz kedvezőtlenek a kiindulási feltételek Európa számára. A kontinens túlságosan sokáig támaszkodott az amerikai kínálatra, előmozdítva az oligopolisták felemelkedését azzal is, hogy polgárai meggondolatlanul hozzájárultak az amerikai *Big Data* adatvagyonához. Ez az adatkincs óriási; túl nagy az amerikaiak időbeli előnye a személyes adatok gyűjtésében: mostanra jó húsz évre rúg.

A mesterséges intelligencia területén is az USA a domináns, de a legígéretesebb versenytársak listáján ugyancsak előkelő helyet foglal el Kína, Dél-Korea, Oroszország, Szingapúr és Izrael.^[28] Európai ország nincs közöttük. Németország ennek ellenére be akar szállni a mesterséges intelligenciáért folyó versenybe, hogy annak „világviszonylatban is vezető székhelyévé váljék”^[29].

Tanácsadóvállalatok megállapították, hogy a mesterséges intelligencia különösen akkor gazdaságos, ha a kiskereskedelemben arra használják, hogy a végfelhasználókat eléggé megkérdőjelezhető módon kategóriákba osszák – fizetőképes, gyen-

ge anyagi helyzetű, egészséges, beteg, jövedelmező, érdeklődő –, és pénzkiadásra ösztönözzék. A mesterséges intelligencia marketing- és értékesítési alkalmazásai azok, amelyek ez idő szerint a legnagyobb forgalmat és legmagasabb profitot érik el – s nem, mondjuk, az ipari felhasználásai. A magyarázat egyszerű. Hét-köznapi tárgyainkkal, az ipari létesítményekkel vagy az infrastruktúrákkal ellentétben az emberek rendelkeznek pénzzel. Aki megfigyeli az embereket, és fogyasztásra tudja csábítani őket, jó üzletet csinál. A tárgyak megfigyelésénél ez másként van. A dolgok nem adnak ki pénzt, ami kihívássá teszi a mesterséges intelligencia üzemgazdasági hasznának meghatározását – tudniillik amikor az „Ipar 4.0” kontextusában válik szükségessé az alkalmazása. Persze előnyös, ha képesek vagyunk egy ipari létesítményt algoritmikusan ellenőrizni és vezérelni. Azonban milyen gazdasági haszna van az ismeretnyereségnek, már ha a mesterséges intelligencia egyáltalán újdonsággal szolgál, és nemcsak azt fedezi fel, amit az üzemeltető már amúgy is tud?

Úgy tisztességes, ha beismerjük: még nem tudni, ki fogja átvenni a vezetést a mesterségesintelligencia-alkalmazások területén. Végül is a piaci rések mindig teremtenek lehetőséget kitérésre. E téren segít a piaci szereplők nem klasszikus módon történő szegmentálása.

A mesterséges intelligencia ökoszisztémáját jelenleg négy terület jellemzi. Ha Németország a mesterséges intelligencia terén globális vezető pozíciót akar szerezni, vajon melyiken tegye? A vezető szerep tudniillik attól a döntéstől is függ, hogy miként akarjuk alkalmazni a technológiát.

Van először is az **algoritmikusok** szegmense. Ők a matematikának, fizikának és informatikának azok a tudósai, akik még a mesterséges intelligencia új eljárásainak vagy elméleteinek kidolgozására is képesek. Ma ez csaknem kizárólag kutatási intézményekben folyik; húsz évvel ezelőtt még vállalatok is tartottak fenn saját fejlesztőcsapatokat. Költségekkel a vállalatok belüli kutatást széles körben leépítették, és az egyetemekre helyezték át. Megállapítható: a német nyelvű kutatók csúcspozíciót töltenek be ott a mesterségesintelligencia-kutatásban.

Igen keserű ürömcsepp azonban, hogy aki elolvassa az európai kutatók legfrissebb publikációit, könnyűszerrel megállapíthatja, honnan érkeztek a harmadik féltől származó finanszírozások. A cikkek végén hosszú listákban szokták felsorolni a kutatások támogatóit, és a finanszírozók ikonikus neveket viselnek. Szembetűnő, hogy mindig ugyanazok szerepelek köztük: a Google, az Amazon, a Facebook. Az általuk finanszírozott európai kutatási eredmények az övék. Ennek köszönhetően Európa inkább a vetélytársainak a mesterségesintelligencia-kutatásban játszott vezető szerepét erősíti, nem pedig saját digitális ökoszisztémáját.

Másodszor, az algoritmikusokból profitálnak a mesterséges intelligencia **vezérszurkolói**, azaz a tanácsadócégek, amelyek gyakran maguk is amerikai gyökerűek. Küzdenek a mesterséges intelligencia interpretációjának monopóliumáért, serkentik a digitális átalakulást és nyomást fejtenek ki a vállalatokra, figyelmeztetve őket: aki ma nem szerelkezik fel mesterséges intelligenciával, a jövőben nem lesz versenyképes. E mögött számítás

húzódik meg, és az a szándék, hogy növeljék a saját forgalmukat és nyereségüket – azáltal, hogy tanácsadási napokat számolnak fel, és ügyfeleiknél szokványos feladatok megoldásához szabadon felhasználható amerikai mesterséges intelligenciát alkalmaznak. A vezérszurkolók nem törekszenek rá, hogy megértsék, miként működik egy harmadik piaci szereplő mesterséges intelligenciája, sem azt, hogy az információ hogyan terjed egy mesterséges neurális hálózatban, illetve hogy ez miért az adott eredménnyel szolgál. Azok is ők, akik azt terjesztik, hogy csak elegendő adatot kell gyűjtenünk és egy mesterséges neurális hálózatba táplálnunk, hogy új felismerésekhez jussunk, mert a mesterséges intelligencia „modelleket dolgoz ki”. Ez megtévesztő, a mesterséges intelligencia ugyanis nem állít fel oksági láncolatokat, ahogyan modelleket sem dolgoz ki – különösen prognózismodelleket nem. Mindössze kölcsönös összefüggéseket fedez fel. Ezek némelyike „szellem-korreláció”, ami semmiféle kapcsolatban nincs a valósággal, amit pedig reprezentálni kívánna.

Harmadszor, a mesterséges intelligencia fekete mágijának urai a **modellezők**,^[30] akik szembenállnak az imént említett empirikusokkal. Alig akad, aki összefüggésbe hozza a mesterséges intelligenciát és a koncepcionális gondolkodókat, ám éppen ők lehetnének a kognitív rendszerek úttörői – a mesterséges intelligencia azon alkalmazásának élharcosai, amelyet a konkurencia csak nagyon nehezen képes másolni, mert a matematikai-szakmai tudás és a gyakorlati tapasztalat egyesül benne. A modellezők azok, akik a korrelációkat, amelyeket a neurális há-

lőzatok produkálnak, tudománytalannak tartják, s inkább azt szeretnék tudni, hogy mi zajlik egy kognitív rendszerben. Munkájuk gazdasági és katonai szempontból nagy jelentőségű. A modellezők ipari folyamatok reprezentációit tudják elkészíteni, amelyek kitűnő eredményeket képesek produkálni. Arra törek-szenek, hogy helyesen alkalmazzák a mesterséges intelligenciát, és hogy az egyetemes technológia teljes eszközkészletét felhasználják. Globális vezérlési rendszereket építenek, melyeknek al-rendszerei lokálisan tevékenykednek, hogy aztán szükség ese-tén együttműködjenek. Ahol észszerű, ott statisztikai becslési el-méleteket, kombinatorikai optimalizációt vagy vezérléelméleti megközelítéseket illesztenek gépi tanulási eljárásokhoz. Munká-juk különösen hasznos a német ipari kultúra számára, hiszen szinte a német génekben gyökerezik, és egyébként különösen adatkímélő. Először modelleznek, azután a modellt azokkal az adatokkal látják el, amelyekre csakugyan szükség is lesz. Ez azonban megfordítva azt is jelenti, hogy az adatok, amelyeket az állam, vagy még kutatóintézetek is tárolnak – azok a fogyasztói adatok pedig mindenképpen, amelyeket az amerikai techno-lógiai óriások két évtized alatt összegyűjtöttek –, az ipar modell-jei számára gyakran használhatatlanok. Ipari adatok nem áll-nak ugyanolyan mennyiségben rendelkezésre, mint személyes adatok – már csak a biztonsági aggályok és a versennyel össze-függő problémák miatt sem.

Egyébként a modellezők is kénytelenek kihívásokkal szem-benézni. Igen alaposan meg kell érteniük az operatív problé-mát, amelyet mesterséges intelligencia alkalmazásával kellene

megoldani. A városi szállítás-logisztikai forgalom optimalizálásához kitűnő logisztikus-matematikusra van szükség, egy rákdiagnosztikai mesterséges intelligenciához tapasztalt orvos-informatikusra. A jövő diplomáciájának pedig technológia-diplomátákra.

„A mesterséges intelligencia a jövő, és nemcsak Oroszország, hanem az egész emberiség számára. Aki ennek a fejlődésnek az élén halad, a világ ura lesz”, mondta Vlagyimir Putyin. Mivel pedig a mesterséges intelligencia tudományos számítás, amihez óriási processzorteljesítmény szükséges, a világ igazi urai azok lesznek, akik a számítógépes infrastruktúrát működtetik. Ezzel eljutottunk a negyedik szegmenshez. Azok, akik a **számítóközpontok** hardverével, a számítógépes felhővel rendelkeznek, a technológiai hatalom birtokosai.

2018-ban a Fujitsu japán számítógépgyártó bejelentette, hogy bezárja egyetlen gyárát, amely még európai földön, Augsburgban hardvert állít elő. Utána nem készül több számítógép Európában. De a modellezők modelljei is jelentős számtástechnikai kapacitást igényelnek. Tanítani kell őket, és számítógép-forrásokra van szükségük, például az Alibaba-felhőre, amely az Amazon-felhőre hasonlít. A mesterséges intelligenciát végső soron az ellenőrzi, aki a hardverhez való hozzáférést engedélyezi vagy megtagadja. Ezzel zárul a kör, és oda jutunk, hogy végső soron az a rendszeralternatíva érvényesül, amely a gazdaságilag releváns forrásokat ellenőrzi. A járadék logikája még a digitális korszakban is előnyösnek bizonyul.

[ZÁRSZÓ]

Amikor az igény találkozik a valósággal

Az általunk ismert Európa túl lassú, túl gyenge, túl kevésbé hatékony. (Emmanuel Macron)

Az előző fejezet tele volt feltételes móddal. Európának demokráciapolitikára *kellene* elszánnia magát; *elengedhetetlen volna*, hogy digitális stratégiáinak ne csak gazdasági, hanem geostratégiai jelentőséget is tulajdonítson, egyaránt törekedve prosperitásra és biztonságra; intézkedéseket *kellene hoznia* az 500 millió digitális környezetben élő európai védelmére; és: innovációs élharcosa *lehetne* azoknak kognitív rendszereknek, amelyek nem egyszerűen tanuló gépek.

Nagy álmom ez egy olyan Európa számára, amelynek a nemzeteit roppantul különböző érdekek vezérlik – legyen szó akár védelmi kérdésekről, akár belső biztonságuk kérdéseiről. Egy olyan Európa víziója, amely maga ad elő egy koherens narratívát, még mielőtt mások tennék meg. Nagyok az elvárások az Európában hegemon szerepet játszó Németországgal szemben, amely gazdasági tekintetben továbbra is kész vezető szerepet

vinni, kényesebb ügyekben azonban jóval kevesebb felelősséget akar vállalni. Olyan technológiastratégia szükségessége fogalmazódik meg benne, amelyet a taktikai és operatív kontextushoz kell igazítani – szembe menve a megszokás restségével, a régi struktúrák közönyével és a társadalom intézményesült folyamataival.

Emlékeznek még a már említett matematikusra, akinek a Pentagon egyik vélhetően brit fedőcége évi 700 ezer dollárt ajánlott fel matematikai tudásáért? Egy német technológus számára az angolszász térségből érkező ajánlat mindig csábító, mert Európa gazdasági motorja, Németország túlságosan tétova az innovációk bevezetésében. Az új technológiák gyakran megrekednek a pokol tornácán, a kísérleti szakaszban. Matematikusunk azonban bajor, kifejezetten lokálpatrióta, s arról álmodozik, hogy nyugdíjas éveit sörcsarnokok asztalai mellett és kártyázással tölti majd. Mivel a külföld minden csábító mesterkedése ellenére sem akar megválni Bajorországtól, nemrégiben az illetékes helyhatóságnál a következő tevékenységi köröket jelentette be vállalkozóként: „IT-tanácsadás, prognosztikus és optimalizációs matematikai modellek fejlesztése, mesterséges intelligencia és kvantum-számítástechnika.”

Mire van szüksége egy matematikusnak egy effajta tevékenységhez? Mindössze egy internetre csatlakoztatható laptop-ra. Munkája alapját a gondolkodás jelenti, az ehhez való nyersanyagot, az adattömegeket a felhőben tárolják, és a sok számolást igénylő munkákat is a számítóközpontok végzik. A matematikus azonban az iparűzési engedély és a szükséges adószám he-

lyett a következő figyelmeztetést kapja: „Ügyében megállapítást nyert, hogy nem rendelkezik építési engedéllyel az iparűzéséhez.” Mesterséges intelligencia Made in Germany – leálló pályára téve a bajor építési szabályzatra hivatkozva, még mielőtt egy kognitív gép koncepciójának első gondolata megfogalmazódott volna. A közigazgatási dokumentum csakugyan e mondattal végződik: „Jelen levelünket továbbítottuk az építésfelügyeleti hatóságnak.”

Németország még mindig nem hallotta meg a startpisztoly hangját. Az Egyesült Államokban felriadtak a világszerte bekövetkező szeizmikus megrázkódtatásoktól, és megállapították: „Ha lemondunk a mesterséges intelligenciáról, használhatatlanná válnak régi védelmi rendszereink, nehéz lesz hozzáférnünk az új piacokhoz, ami pedig jólétünk és életszínvonalunk biztosítója, és kárát látja az együttműködés szövetségeseinkkel és partnereinkkel, akik pedig erre alapozták saját személyes szabadságukat.”^[1] Németország viszont, úgy tűnik, szilárdan meg van győződve arról, hogy a továbbiakban is minden úgy megy tovább, ahogyan eddig.

„Az amerikaiak nem vonulnak ki a világ történeteiből” veti ellene ezért a Bundeswehr egyik katonája annak a tételnek, hogy az amerikaiak meg akarnak szabadulni eddigi felelősségüktől. „Épp ellenkezőleg, fegyverkeznek. A Dél-kínai-tengerre három repülőhordozót küldtek.” Ez utóbbi igaz, mert egy kínai tengernagy azzal fenyegetődött, hogy kettőt közülük elsüllyesztenek,^[2] és az is helytálló, hogy a britek saját repülőhordozójukat a csendes-óceáni geostratégiai törésvonalnak arra a részére

küldték,^[3] abba a konfliktusövezetbe, ahol majd eldől, hogy a 21. században melyik rendfenntartó hatalom lesz meghatározó – Európa számára is. Az, hogy Amerika ott demonstrálja katonai erejét, ahol döntő fontosságú dolgok történnek, nem mond el-lent az USA visszavonulásának – aminek oka, hogy nem akarja tovább egymaga finanszírozni az egyre drágábbá váló közjava-kat.

Ha megkérdezzük a véleményét, a német katona, a helyi né-met közigazgatás és számos polgár még nem egészen tudja hova tenni azt a lendületet, amivel a világ rendjének átalakulása vég-bemegy. Ennek az áttörésnek a során a digitális technológiák döntő szerepet játszanak, szolgáljanak bár a politikai ellenőrzés megtartására vagy a katonai erőszak eszközeiként. Közéjük tar-toznak a szűnni nem akaró támadások az európai számítógé-pek, bankszámlák, és a felhasználók feje ellen. Az IT-közeli vál-lalkozások, mint például a telekommunikációs szolgáltatók, ke-ményen dolgoznak, hogy e támadások következményei kiszá-míthatók maradjanak. Ekképpen a lakosság túlnyomó része szá-mára nemcsak láthatatlanok maradnak, hanem legtöbbször a személyes következményeiket sem szenvedik el.

Ezzel együtt komolyan kell venni őket. Cyberháború? Rend-szerkiesés? Hálózatra kötött amerikai nukleáris fegyverek meg-hekkelése katasztrofális következményekkel? A támadó politi-kai szándéka szerinti digitális pusztítás akkor is elképzelhető, ha már az állandó szurkálások elegendők, hogy alattomosan aláássák egy digitális társadalomnak a hálózatosításba, követke-zésképpen a demokratikus állam azon képességébe vetett bizal-

mát, hogy gondoskodni tud a biztonságról. Még nincs szó háborúról, és bejelentett háború nem is folyik. Emberéleteket sem kell gyászolnunk. A digitális 21. század technológiái azonban megteremtik a lehetőséget, hogy a nemzetek ismét összemérjék erőiket. Terjed a béke törékenységének, a fenyegetés növekedésének az érzése. Maguktól értetődő dolgok már nem maguktól értetődők. Valami nem stimmel. Valami nem kerek. Az egyes emberek és a világ közti kapcsolatok labilissá váltak. Szó szerint nő a bizonytalanság és vele a szkepszis a kormányokkal és az állam hatalmi monopóliumával szemben. De éppen a félelem az a humusz, amin a populizmus virágzik, az pedig kiélez, polarizál és radikalizál. Ha megállapodott pártok populisztikus tartalmakat tesznek magukévá, hogy ezzel választói szavazatokat szerezzenek, a demokrácia máris kárt szenvedett anélkül, hogy akár egyetlen lövést leadtak volna.

A digitalizáció egykor sokat ígérő volt, és a gazdaság meg a tanácsadói még mindig himnuszokat zengenek a mesterséges intelligenciáról, a digitális közgazdaságtanról és a következő generációs üzleti modellekről, mintha minden a régi volna. A digitális haladás feletti uralmat azonban nem hagyhatjuk rá egyedül a gazdaságra, mert a digitalizáció nem csak a jobb technológia és teljesítőképesebb gazdaság dimenziójával rendelkezik. Új államközi konfliktusok potenciálját is magában hordja. Olyan konfliktusokét, amelyek mindannyiunkat személy szerint érintenek, mert életünk békéjét és biztonságát kérdőjelezi meg. A digitális korban nem maradhat vakfolt a biztonság, de csak akkor tárhatjuk fel, ha a továbbiakban nem térünk ki a Németer-

szág és Európa 21. századi biztonságáról folytatandó nemszeretem vita előtt.

Csak afelett lehet hatalmunk, amit értünk.

Köszönetnyilvánítás

A jelen szöveget azok inspirálták, akik megosztották velem idejüket és jelentős tudásukat: nagyra becsült interjúalanyaimtól kaptam a legértékesebb impulzusokat mind a forma, mind a tartalom tekintetében. Álljon itt a nevük ábécé-sorrendben:

Michael Biontino nagykövet, Dr. Heiko Borchert, Stefan C. P. Hinz vezérkari ezredes, Wolfgang Ischinger nyugalmazott nagykövet, Dr. Wolfgang Koch, a Szövetségi Alkotmányvédelmi Hivatal nyugalmazott elnöke, Hans-Georg Maaßen, Dr. Ulrich Menzel nyugalmazott professzor, Dr. Jean-Marc Rickli, Dr. Christina Schori Liang és Tobias Vestner.

Genfnek kettős arca van. Amellett, hogy a pénzügyek híres központja, számos nemzetet egyesítő szervezet vendéglátója is. Külön köszönettel tartozom Stefan Hinz ezredesnek, aki a Bundeswehr Genfi Biztonságpolitikai Központhoz delegált képviselőjeként szívélyes fogadtatásban részesített, közvetítőként és szervezőként pedig szakértőkkel folytatott beszélgetéseket tett lehetővé számomra.

Nagy segítségemre volt Toni Dahmen százados, a wahni Luftwaffe csapatparancsnokság tisztje, Dr. Joachim Keppler, aki a többfázisú zavaróradar véletlen felfedezésének történetét fizikai szempontból ellenőrizte és korrigálta, és Dr. Christian

Brandlhuber, aki tudományos pályafutása során anekdoták szinte kimeríthetetlenül gazdag tárházára tett szert.

A legnagyobb köszönet illeti kedves barátomat, Dr. Friedrich von Westphalen professzort, aki nemcsak ügyvédi szakértelmét vetette latba, hogy ellenőrizze a nemzetközi jog területén tett kalandozásaimat, hanem saját, évtizedes újságírói tapasztalatai alapján figyelmeztetett is: „Ugrál az igeidők között!”

Mindannyian egytől egyig szívesen korrigálták, amit közléseikből levezettem. Érzésem szerint jó néhány száz e-mailt váltottunk. Ezzel együtt a szövegben esetleg bent maradt minden hibáért egyedül engem terhel a felelősség.

Jegyzetek

[ELŐSZÓ]

A béke kellős közepén

- 1 Bing, 2018
- 2 Ehhez részletesen: Rickli & Krieg, 2018, 115. o.
- 3 Uo.

[EGY]

A kód mint fegyver

- 1 United States District Court, 2017, 8. o.
- 2 Bossert, 2017
- 3 BBC News, 2017
- 4 Uo.
- 5 Vita Manuel Koschuch okl. mérnökkel a „Beszélgetés a jövőről” munkacsoportban, 2017. nov. 23., Fachhochschule Campus, Bécs (részlet)
- 6 Tucker, NSA Chief: Rules of War Apply to Cyberwar, Too, 2015
- 7 Smith B., 2017
- 8 Uo.
- 9 Arendt, Die Freiheit, frei zu sein, 2018, 11. o.
- 10 van Creveld, 2017, 17. o.

- 11 Arendt, On Violence, 1969, 9. o.
- 12 von Clausewitz, 1832–1834, 15. o.
- 13 Gray, 2015, 17.
- 14 Arendt, On Violence, 1969, 35. o.
- 15 Uo., 56. o.
- 16 Schäffle, 1897, 589. o.
- 17 Mills, 1956, 171. o.
- 18 Arendt, On Violence, 1969, 11. o.
- 19 Gabriel S., 2018
- 20 Simms & Laderman, 2017, 29. o.
- 21 Arendt, On Violence, 1969, 9. o.
- 22 Harari, 2017, 28. o.
- 23 Gray, 2015, 22. o.
- 24 Prisching, 2017, 344. o.
- 25 Ischinger, Interjú Wolfgang Ischingerrel, 2018, 10.1. hivatk.
- 26 Snyder, Über Tyrannei, 2017, 42. o.
- 27 Ischinger, Interjú Wolfgang Ischingerrel, 2018, 17. hivatk.
- 28 Ehhez részletesen: Münkler, Die neuen Kriege, 2004
- 29 Ischinger, Interjú Wolfgang Ischingerrel, 2018, 8. hivatk.
- 30 Nolte, 2018, 115. o.
- 31 Uo., 116.
- 32 Uo.
- 33 Münkler, Die neuen Kriege, 2004, 11. o.
- 34 Uo., 7.

- 35 Rickli, Interjú Jean-Marc Ricklivel, 2018, 82. hivatk.
- 36 Uo., 72. hivatk.
- 37 A potyautassághoz vö. Menzel, *Die neue eurasische Weltordnung*, 2018, 51–53.
- 38 „Because the truth is, under President Obama we’ve lost control of things that we used to have control over. We came in with an internet, we came up with the internet. And I think Secretary Clinton and myself would agree very much, when you look at what ISIS is doing with the internet, they’re beating us at our own game.” Sottek, 2016
- 39 Hayden, 2018, 15. o.
- 40 Horowitz, Allen, Kania, & Scharre, 2018, 3. o.
- 41 2018. augusztus 3-án az Apple piaci értéke először haladta meg az egymilliárd dollárt.
- 42 Simms & Laderman, 2017, 21. o.
- 43 Uo.
- 44 Emmott & Wroughton, 2018
- 45 Specia, 2018
- 46 Rickli, Interjú Jean-Marc Ricklivel, 2018, 1. hivatk.
- 47 Azzellini, 2006
- 48 Uo.
- 49 Kilcullen, 2015, 133. o.
- 50 Arendt, *On Violence*, 1969, 48. o.
- 51 Rickli, Interjú Jean-Marc Ricklivel, 2018, 11. és 12. hivatk.
- 52 Ischinger, Interjú Wolfgang Ischingerrel, 2018, 93. hivatk.

- 53 Uo., 98. hivatk.
- 54 Hofstetter, 2016, 28. és 50. o.
- 55 Brennan, 2017
- 56 Rickli, Interjú Jean-Marc Ricklivel, 2018, 17. és 19. hivatk.
- 57 Brennan, 2017
- 58 Rickli, Interjú Jean-Marc Ricklivel, 2018, 107. hivatk.
- 59 Galeotti, 2014
- 60 Calabresi, 2018, 34. o.
- 61 Uo.
- 62 Sepulvado, 2017
- 63 Sainato, 2016
- 64 Horseman, 2016
- 65 Brennan, 2017
- 66 Uo.
- 67 Calabresi, 2018, 36. o.
- 68 A *TIME* Cybersecurity-különkiadása, „Hacking, the Dark Web and You” címen. A *TIME*-ban e témában megjelent cikkek gyűjteménye. „The Secret History of an Election” című írásából az alábbi bekezdés maradt ki: „From the first report of Russian hacking in mid-June, Donald Trump denied Moscow’s involvement, improbably accusing the Democratic National Committee of hacking itself ‘as a way to distract from the many issues facing their deeply flawed candidate and failed party leader.’ As the story accelerated with the dump of stolen emails right before the Democratic National Convention, Trump doubled down on his counterclaims. On Aug. 1 in Co-

lumbus, Ohio, he said, ‘I’m afraid the election is going to be rigged.’ Letöltve innen, 2018. június 20.:

<http://time.com/4865982/secret-plan-stop-vladimir-putin-election-plot/> ;

69 Tucker, You Have 19 Minutes to React If the Russians Hack Your Network, 2019

70 Brennan, 2017

71 Calabresi, 2018, 39. o.

72 Uo.

73 Brennan, 2017

74 Uo.

75 Uo.

76 Uo.

77 Calabresi, 2018, 36. o.

78 Brennan, 2017

79 „I don’t think Russian intelligence chiefs want to go beyond their ski tips, as far as what it is that they are doing that could escalate and spiral. So I do think things such as that, or to engage in an election that could have some real significant repercussions, I am confident, very confident, that they would have run those things by Mr. Putin. The actual details of how it would be implemented is something that I think Mr. Putin would leave to his intelligence chiefs, but the ›go‹ signal, the green light would have come from Mr. Putin”, Brennan, 2017

80 Calabresi, 2018, 38. o.

81 Starks, 2017

- 82 Calabresi, 2018, 38. o.
- 83 Uo., 40. o.
- 84 Uo.
- 85 Starks, 2017
- 86 Rickli, Interjú Jean-Marc Ricklivel, 2018, 29. hivatk.
- 87 Maurer, 2018, 23. o.
- 88 Uo., 24. o.
- 89 Ischinger, Interjú Wolfgang Ischingerrel, 2018, 26. hivatk.
- 90 „My people came to me – Dan Coats came to me and some others – they said they think it’s Russia. I have President Putin; he just said it’s not Russia. I will say this: I don’t see any reason why it would be.” Fehér Ház, 2018
- 91 Rickli, Interjú Jean-Marc Ricklivel, 2018, 40. hivatk.
- 92 Uo., 64. hivatk.
- 93 Uo., 65. hivatk.
- 94 Uo., 67. hivatk.
- 95 United States District Court, 2018, 1. o.
- 96 The New York Times, 2018
- 97 Ehhez részletesen: Perkins, 2016
- 98 United States District Court, 2018, 10. o.
- 99 Vö. <https://aws.amazon.com/de/stateandlocal/election-as-a-service/>
- 100 Coats, Dialogues on American Foreign Policy and World Affairs: Director of National Intelligence Dan Coats and Walter Russell Mead, 2018

- 101 Uo.
- 102 Kovacs, 2018
- 103 Német technológiai konszern menedzserének a szerző előtt tett kijelentése a létesítményirányítás mesterséges intelligencia alapú optimalizálásáról folytatott beszélgetés során.
- 104 Német közlekedési konszern menedzserének a szerző előtt tett kijelentése a közlekedési infrastruktúra mesterséges intelligencia alapú ellenőrzéséről folytatott beszélgetés során.
- 105 Dillet, 2018
- 106 A „Beszégetés a jövőről” munkacsoportban folytatott eszmecsereből, 2017. nov. 23., Fachhochschule Campus, Bécs
- 107 Bob, 2018
- 108 Bundesamt für Verfassungsschutz, 2018, 2. o.
- 109 Wirtschaft.com, 2018
- 110 Smith R., 2018
- 111 Maaßen, Interjú Hans-Georg-Maaßennel, 2018, 27. hivatk.
- 112 Uo., 28. hivatk.
- 113 Uo., 29. és 32. hivatk.
- 114 Borchert, 2018, 13. hivatk.
- 115 Borchert, 2018, 17. hivatk.
- 116 Maaßen, Interjú Hans-Georg-Maaßennel, 2018, 40. hivatk.
- 117 Allan, 2018
- 118 G20, 2017
- 119 Maurer, Levite, & Perkovich, Toward a Global Norm Against Manipulating the Integrity of Financial Data, 2017, 11. o.

- 120 Das & Spicer, 2016
- 121 Maurer, Levite, & Perkovich, Toward a Global Norm Against Manipulating the Integrity of Financial Data, 2017, 1 o.
- 122 Maaßen, Interjú Hans-Georg-Maaßennel, 2018, 104. hivatk.
- 123 Uo., 105. hivatk.
- 124 Paquette, 2015
- 125 Uo.
- 126 Mansholt, 2018
- 127 Guardian staff and agencies, 2018
- 128 Tucker, How NATO Is Preparing to Fight Tomorrow’s Information Wars, 2017
- 129 Feinberg, 2018
- 130 Coats, Dialogues on American Foreign Policy and World Affairs: Director of National Intelligence Dan Coats and Walter Russell Mead, 2018

[KETTŐ]

Információs háború

- 1 Ischinger, Előadás; Bayerischer Hof, München: Zukunftsfragen deutscher und europäischer Sicherheitspolitik, 2017
- 2 Uo.
- 3 ZDF heute, 2017
- 4 Snowden, 2018
- 5 2016. júniusi cégértékelés; 2016. novemberi felhasználószámok (kerekítve)

- 6 Vö. ehhez: Martínez, 2016
- 7 Kobek, 2016, 82. o.
- 8 Uo.
- 9 Vö. A Német Szövetségi Köztársaság Alaptörvénye, 21. cikkely, I. bek, 1. o.
- 10 „The U.S. intelligence community is confident the Russian government directed the recent compromise of emails from U.S. persons and institutions. These thefts and disclosures are intended to interfere with the U.S. election process. Russia’s senior-most officials are the only ones who could have authorized the activities.”, Woodward, 2018, 29.
- 11 Office of the Director of National Intelligence, 2017, 3. o.
- 12 Office of the Director of National Intelligence, 2017, 3. o.
- 13 Uo., 200. o.
- 14 United States District Court, Februar 2018, 6. o.
- 15 Office of the Director of National Intelligence, 2017, ii. o.
- 16 Rid, 2018, 216. o.
- 17 Google Books Ngram Viewer, 2018
- 18 Rid, 2018, 200. o.
- 19 „We are all peering eagerly into the future to try to forecast the action of the great dumb forces set in operation by the stupendous industrial revolution which has taken place during the present century. We do not know what to make of the vast displacements of population, the expansion of the towns, the unrest and discontent of the masses, and the uneasiness of

those who are devoted to the present order of things.” Roosevelt, 1924, 107. o.

- 20 II. Vilmos császár 1914. augusztus 6-i beszéde
- 21 Ferguson, 2018, 473. o.
- 22 Ferguson, 2018, 473. o.
- 23 Calamur, 2017
- 24 Salisbury, 2017
- 25 Bidder, 2017
- 26 Ischinger, Interjú Wolfgang Ischingerrel, 2018, 3. és 5. hivatk.
- 27 McLuhan, 1970, 66. o.
- 28 Ehhez részletesen: Singer & Brooking, 2018
- 29 Woodward, 2018, 23. o.
- 30 Uo., 25. o.
- 31 Zeit online, 2018
- 32 „The information space opens wide asymmetrical possibilities for reducing the fighting potential of the enemy.” Gerasimov, 2013
- 33 DeGeurin, 2018
- 34 Lobe, 2018
- 35 Garamone, 2018
- 36 Thomas, 2004, 237.
- 37 Arendt, Wahrheit und Lüge in der Politik. Zwei Essays, 1972, 40. o.
- 38 Uo., 60. o.
- 39 Uo., 60. o.

- 40 Uo., 50. o.
- 41 Eichmeier, 2018, 3. o.
- 42 Patrikarakos, 2017, 27. o.
- 43 Uo., 29. o.
- 44 Prose, 2015
- 45 Scott, 1921
- 46 Arendt, Elemente und Ursprünge totaler Herrschaft, 1951, 682. o. (A totalitarizmus gyökerei, 388. o.)
- 47 Uo., 696. o. (A totalitarizmus gyökerei, 394. o.)
- 48 Uo., 694. o. (A totalitarizmus gyökerei, 393. o.)
- 49 Az informatikusok valami egészen mást értenek a szingularitás fogalmán: azt az időpontot írja le, amelyben egy mesterséges intelligencia meghaladja az emberi intelligenciát.
- 50 Arendt, Elemente und Ursprünge totaler Herrschaft, 1951, 685. o.
- 51 Vö. ehhez: Dörr & Natt, 2014
- 52 Arendt, Elemente und Ursprünge totaler Herrschaft, 1951, 679. o. (A totalitarizmus gyökerei, 386. o.)
- 53 Luhman, 1994
- 54 Hayden, 2018, 48. o.
- 55 Nichols, 2017, 3. o.
- 56 Uo., 28. o.
- 57 Ehhez részletesen: Ferguson, 2018, 55–60. o.
- 58 Uo., 37. o.
- 59 Uo., 35. o.

- 60 Arendt, Elemente und Ursprünge totaler Herrschaft, 1951, 679. o.
- 61 Más intézmények – egyesületek, egyházak – hasonló tapasztalatokra tesznek szert, amelyek nem vezethetők vissza kizárólag demográfiai változásokra vagy botrányos magatartásra adott reakciókra.
- 62 Arendt, Elemente und Ursprünge totaler Herrschaft, 1951, 695. o. (A totalitarizmus gyökerei, 393. o.)
- 63 Így járt el Adolf Hitler, vö. Arendt, Elemente und Ursprünge totaler Herrschaft, 1951, 699. o.
- 64 Így járt el Joszif Sztálin, vö. Arendt, Elemente und Ursprünge totaler Herrschaft, 1951, 699. o.
- 65 Ehhez részletesen: Hayden, 2018, de ugyanígy: Woodward, 2018
- 66 Fredericks, 2018
- 67 Arendt, Elemente und Ursprünge totaler Herrschaft, 1951, 695. o. (A totalitarizmus gyökerei, 393. o.)
- 68 Uo., 677. o.
- 69 Uo., 678. o.
- 70 Trump, An open letter from Donald J. Trump, 1987
- 71 Trump, beszéd: Donald Trump Holds a Political Rally in Wilkes-Barre, PA, 2018
- 72 Trump, beszéd: Donald Trump in Minneapolis, MN, 2016
- 73 Trump, beszéd: Donald Trump Holds a Make America Great Again Rally in Tampa, 2018

- 74 Trump, Interjú: Jeff Glor Interviews Donald Trump in Scotland (Complete), 2018
- 75 Hamilton, 1787
- 76 Az események ismertetése Eberlein dokumentumfilmes összefoglalóján alapul, 2018
- 77 Ehhez részletesen: Stangl, 2011
- 78 Uo.
- 79 Eberlein, 2018, a 01:01:30. percnél
- 80 Polizei Bayern, 2017
- 81 Backes, Jaschensky, Langhans, Munzinger, Witzenberger & Wormer, 2016
- 82 Eberlein, 2018, a 00:32:31 percnél
- 83 Uo., a 00:32:14 percnél
- 84 Uo., 00:32:14 percnél
- 85 Idézve Prisching nyomán, 2017, 339. o.
- 86 Ehhez részletesen: Ries, Bersoff, Armstrong, Adkins, & Bruening, 2018
- 87 Tett, 2016
- 88 Arendt, Elemente und Ursprünge totaler Herrschaft, 1951, 668–670. (A totalitarizmus gyökerei, 381–382. o.)
- 89 Inglehart & Norris, 2016, 6.
- 90 Newman, Fletcher, Kalogeropoulos, Levy, & Nielsen, 2018, 10. és köv.
- 91 „Believe in truth. To abandon facts is to abandon freedom. If nothing is true, then no one can criticize power, because there

is no basis upon which to do so. If nothing is true, then all is spectacle. The biggest wallet pays for the most blinding lights.” Snyder, Goodreads, dátum nélkül.

- 92 Egy fiatalember a szerzőhöz, egy rendezvényen.
- 93 Langner, 1969, 282. o.
- 94 Uo., 283. o.
- 95 Uo., 279. o.
- 96 Horn, 2008, 119. o.
- 97 Ischinger, Interjú Wolfgang Ischingerrel, 2018, 121., 126. és 127. hivatk.
- 98 Uo., 120. hivatk.
- 99 Arendt, Elemente und Ursprünge totaler Herrschaft, 1951, 840. o.
- 100 Hayden, 2018, 78. o.
- 101 Schmidt, 2018
- 102 United States District Court, 2018, 7. o.
- 103 Brennan, 2017
- 104 Meadows, 2017, 5. o.
- 105 Rickli, Interjú Jean-Marc Ricklivel, 2018, 122. hivatk.
- 106 Arendt, Wahrheit und Lüge in der Politik. Zwei Essays, 1972, 10. o.
- 107 Uo., 50. o.
- 108 Ehhez részletesen: Gabriel M., Ich ist nicht Gehirn, 2015
- 109 Rickli, Interjú Jean-Marc Ricklivel, 2018, 120. hivatk.
- 110 Uo., 113. és 114. hivatk.

- 111 Kissinger, 2018
- 112 Rickli, Interjú Jean-Marc Ricklivel, 2018, 116. és 113. hivatk.
- 113 Uo., 118. hivatk.
- 114 Borchert, 2018, 115. és 116. hivatk.
- 115 Becker-Wenzel & Beuscher, 2018, 06:15. perc
- 116 Uo., 04:40. perc
- 117 Lásd még a 2018-as chemnitzi vagy a 2018. szeptember 9-iki, kötheni eseményeket, ahol egy megrendezett „gyászfelvonulás” békésen kezdődött, ám az erőszak eszkalációját (miután résztvevők nemzetiszocialista jelszavakat skandáltak), csak a polgármester és a rendőrség akadályozta meg.
- 118 Ruhani iráni elnöknek: „NEVER, EVER THREATEN THE UNITED STATES AGAIN OR YOU WILL SUFFER CONSEQUENCES THE LIKES OF WHICH FEW THROUGHOUT HISTORY HAVE EVER SUFFERED BEFORE. WE ARE NO LONGER A COUNTRY THAT WILL STAND FOR YOUR DEMENTED WORDS OF VIOLENCE & DEATH. BE CAUTIOUS!”
- 119 „The Iran sanctions have officially been cast. These are the most biting sanctions ever imposed, and in November they ratchet up to yet another level. Anyone doing business with Iran will NOT be doing business with the United States. I am asking for WORLD PEACE, nothing less!”
- 120 Coldewey & Hatmaker, 2017
- 121 Zeit online, 2017
- 122 Wike, Stokes, Poushter, Silver, Fetterolf & Devlin, 2018

- 123 General (Ret.d) Allan, General (Ret.d) Breedlove, Lindley-French, & Admiral (Ret.d) Zambellas, 2017, 12. o.
- 124 „Real power is, I don't even want to use the word, fear.”
Trump, Interjú: Woodward, Costa Interjúja Donald Trumppal.
The Washington Post, 2016
- 125 Woodward, 2018, 175. o.
- 126 Ischinger, Welt in Gefahr, 2018, 126. o.

[HÁROM]

Fegyverkezési verseny a mesterséges intelligencia területén

- 1 Horowitz, Allen, Kania, & Scharre, 2018, 5. o.
- 2 Siegele, 2018, 13. o.
- 3 Ministry of Defence, 2018, 6. o.
- 4 Geiß, Die völkerrechtliche Dimension autonomer Waffensysteme, 2015, 4. o.
- 5 McKinsey&Company, dátum nélkül
- 6 Rickli, Interjú Jean-Marc Ricklivel, 2018, 55. hivatk.
- 7 Koch W., a szerző egy e-mail-jéből, 2018
- 8 Vö. Koch W., On Detecting Radiological Bombs With Potential Applications to Field Camp and Soldier Protection, 2018
- 9 Idézi: Koch W., Menschliche Verantwortung als Leitgedanke für technisches Design bei FCAS. Draft V0.3, 2019, 2. o.
- 10 Biermann & Wiegold, 2015, 17. o.
- 11 Vö. International Monetary Fund, 2018
- 12 AFP news agency, 2018

- 13 CNN Wire Staff, 2011
- 14 Rickli, Interjú Jean-Marc Ricklivel, 2018, 56. hivatk.
- 15 Uo., 58. hivatk.
- 16 Federal Aviation Association, 2016
- 17 Rickli, Interjú Jean-Marc Ricklivel, 2018, 57. hivatk.
- 18 Siegele, 2018, 10. o.
- 19 Defense One Radio, 2018
- 20 Koch W., Künstliche Intelligenz? Die Algorithmenwelt und menschliche Verantwortung, 2018, 50. o.
- 21 Uo., 45. o.
- 22 Stewart, 2018
- 23 Drevstad, 2012, 7. o.
- 24 Campaign to Stop Killer Robots, 2018
- 25 General (Ret.d) Allan, General (Ret.d) Breedlove, Lindley-French, & Admiral (Ret.d) Zambellas, 2017, 3. o.
- 26 CDU, CSU és SPD, 2018, 7062. és köv. sorok
- 27 Vestner, 2018, 17. hivatk.
- 28 Uo.
- 29 Wolfgang Koch és a szerző beszélgetése nyomán
- 30 Department of Defense, 2012, 13. o.
- 31 Geiß, Lethal Autonomous Weapon Systems. Technology, Definition, Ethics, Law & Security, 2014, 3. o.
- 32 Giacca, 2014, 119. o.
- 33 Welt, 2018

- 34 Boyd, 2018
- 35 Vestner, 2018, 21. hivatk.
- 36 Sauer, 2018, 2. o.
- 37 Uo., 3.
- 38 Giacca, 2014, 120–124. o.
- 39 Uo., 125. o.
- 40 Hellestveit, 2014, 140. o.
- 41 Gabriel M., Der Sinn des Denkens, 2018, 52. o.
- 42 Kalmanovitz & Pablo, 2014, 190. és következők
- 43 A német Luftwaffe 43+17 Tornado IDS-T 4017/GT-014 taktikai azonosítójú Tornadói Manchingban állomásoznak. Vö. <https://www.flugzeugforum.de/threads/bw-kennungen-seit-1968.62214/page-3>
- 44 Frequenzplan der Bundesnetzagentur, 2016
- 45 Koch W., e-mail a szerzőnek, 2018
- 46 Theuretsbacher, 2014
- 47 NASA, 2014

[NÉGY]

Visszahekkelés

- 1 Panetta, 2012
- 2 Tucker, Major Cyber Attack Will Cause Significant Loss of Life By 2025, Experts Predict, 2014
- 3 Sanger, 2018, 43. o.

- 4 Maaßen, Interjú Hans-Georg Maaßennel, 2018, 47. és 43. hivatk.
- 5 Vestner, 2018, 24. hivatk.
- 6 Uo., 30. hivatk.
- 7 Borchert, 2018, 94. hivatk.
- 8 Maaßen, Interjú Hans-Georg-Maaßennel, 2018, 33. hivatk.
- 9 Vestner, 2018, Zitat 35. hivatk.
- 10 Maaßen, Interjú Hans-Georg-Maaßennel, 2018, 45. hivatk.
- 11 Uo., 40. hivatk.
- 12 Tanriverdi, 2018
- 13 Münkler, Die neuen Kriege, 2004, 42. o.
- 14 Carvin & Williams, 2015, 188. o.
- 15 Az emberi jogok megsértésének másik példája a Guantanamo Bay-i fogolytábor. Az Egyesült Államok, vezető globális rendfenntartó hatalmi státuszára hivatkozva (amelynek autonómiafelfogásához hozzátartozik, hogy kifejezetten kivonja magát a nemzetközi jog hatálya és a független igazságszolgáltatás illetékessége alól), megnehezíti a hágai nemzetközi büntetőbíróság munkáját, amikor ez amerikai állampolgárok ellen feltételezhető háborús bűncselekmények miatt nyomoz.
- 16 Carvin & Williams, 2015, 23. o.
- 17 Uo., 5. o.
- 18 Arendt, On Violence, 1969, 6. o.
- 19 Carvin & Williams, 2015, 67. o.
- 20 Nolte, 2018, 112. o.

- 21 Münkler, Hybrid Wars. The Dissolution of the Binary Order of V
and Peace, and Its Consequences, 2015, 20. o.
- 22 Vestner, 2018, 32. hivatk.
- 23 Westphalen, 1971
- 24 Tucker, How NATO Is Preparing to Fight Tomorrow's Informa-
tion Wars, 2017
- 25 NATO, 2014, 13. sz.
- 26 Vö. Arendt, On Violence, 1969
- 27 Uo., 36.
- 28 Carvin & Williams, 2015, 46. o.
- 29 Az ENSZ Alapokmánya, 2. cikkely 4. bek.
- 30 Dörr O., 2004
- 31 Az ENSZ Alapokmánya, 51. cikkely
- 32 Uo.
- 33 International Group of Experts at the Invitation of the NATO
Cooperative Cyber Defence Centre of Excellence, 2017, Rule
73, 352. o.
- 34 Uo., 563. o.
- 35 Foltz, 2012, 43. o.
- 36 Sanger, 2018, 49. o.
- 37 Vö. <https://sicherheitstacho.eu/start/main>
- 38 Vestner, 2018, 29. hivatk.
- 39 Rid, 2018, 257. o.
- 40 Dörr O., 2004
- 41 Foltz, 2012, 46. o.

[ÖT]

Harc a dominanciáért

- 1 „Does the USA want to be the Policeman of the Middle East, getting NOTHING but spending precious lives and trillions of dollars protecting others who, in almost all cases, do not appreciate what we are doing? Do we want to be there forever? Time for others to finally fight...”, Trump, #realdonald-trump, 2018
- 2 Menzel, Die Ordnung der Welt, 2015, 869. o.
- 3 Menzel, Interjú Ulrich Menzellel, 2018, 123. hivatk.
- 4 The Economist, 2018
- 5 Ehhez részletesen: Menzel, Die Ordnung der Welt, 2015
- 6 Személyes közlés a szerzőnek adott interjú alkalmával
- 7 Menzel, Interjú Ulrich Menzellel, 2018, 36. hivatk.
- 8 Uo., 41. hivatk.
- 9 Hofstetter, 2016, 63–68.
- 10 V.ö.: <https://www.emojione.com/>
- 11 Zuboff, 2018, 118. o.
- 12 Menzel, Interjú Ulrich Menzellel, 2018, 78. hivatk.
- 13 Sokolov, 2018
- 14 Menzel, Interjú Ulrich Menzellel, 2018, 46. hivatk.
- 15 Menzel, Interjú Ulrich Menzellel, 2018, 37.1. hivatk.
- 16 A teljesség kedvéért említettessék meg: Ulrich Menzel kifejezetten utal arra, hogy a járadékbevételeknek ugyancsak jövedelmet generáló forrásai a fejlesztési segélyek, amelyeknek egy

részét korrump gengszterek kapják meg, hogy egyáltalán hozzájáruljanak a segélyezéshez, [ugyanígy] az [ember]csempészeknek migránsok által fizetett pénzek, továbbá a váltságdíjak, amelyeket kalózok kezére került teherhajókért fizetnek ki.

- 17 Menzel, Interjú Ulrich Menzellel, 2018, 38. hivatk.
- 18 Uo., 118. hivatk.
- 19 Trump, beszéd: Donald Trump in Waterloo, IA, 2015
- 20 Menzel, Die neue eurasische Weltordnung, 2018, 51. o.
- 21 Gabriel S., 2018
- 22 Silver, 2018
- 23 Menzel, Interjú Ulrich Menzellel, 2018, 42. hivatk.
- 24 Menzel, Interjú Ulrich Menzellel, 2018, 48. hivatk.
- 25 Mortensen, 2017
- 26 <https://tradingeconomics.com/united-states/gdp>
- 27 Central Intelligence Agency, 2019
- 28 Stockholmi Nemzetközi Béke kutató Intézet, SIPRI, 2018
- 29 Saját számítások nyilvánosan hozzáférhető adatbázisok alapján (pl. Világbank és Trading Economics)
- 30 Browder, 2016, 79. o.
- 31 Uo., 112. o.
- 32 Trenin, 2017
- 33 Pearson, 2017, 4. o.
- 34 Carlin, 2018
- 35 Inozemtsev, 2018, 51. o.
- 36 Steiner, 2018

- 37 ENSZ Kereskedelmi és Fejlesztési Értekezlete, 2018, 37. o.
- 38 Menzel, Interjú Ulrich Menzellel, 2018, 2. és 3. hivatk.
- 39 Lepault & Franklin, 2018, 01:30. perc
- 40 Weigel, 2003, 237. o.
- 41 A Kínai Kommunista Párt Közp. Bizottsága, 2013
- 42 Siegele, 2018, 10. o.
- 43 Menzel, Interjú Ulrich Menzellel, 2018, 137. hivatk.
- 44 Ehhez részletesen: Menzel, Die neue eurasische Weltordnung, 2018
- 45 Menzel, Interjú Ulrich Menzellel, 2018, 20. hivatk.
- 46 Uo., 19. hivatk.
- 47 Mayer-Kuckuk, 2018, 39. o.
- 48 Menzel, Interjú Ulrich Menzellel, 2018, 86. hivatk.

[HAT]

„Csak feltételesen védekezésre kész”

- 1 Swan & McCammond, Why Trump swears off planning, 2019
- 2 Swan, Trump’s strategic planning inspiration: Mike Tyson, 2019
- 3 Anonym, 2018
- 4 Menzel, Die Ordnung der Welt, 2015, 888. o.
- 5 Pompeo, 2018
- 6 Scholz, 2018

- 7 Ischinger, Előadás a Bayerischer Hofban, München: Zukunftsfragen deutscher und europäischer Sicherheitspolitik, 2017
- 8 Lásd még ezzel kapcs.: Menzel, Die Ordnung der Welt, 2015, 958. o.
- 9 Vö. Stocker, 2019
- 10 Ischinger, Előadás a Bayerischer Hofban, München: Zukunftsfragen deutscher und europäischer Sicherheitspolitik, 2017
- 11 Bundesakademie für Sicherheitspolitik; Auswärtiges Amt & Heinrich-Böll-Stiftung, 2019
- 12 Szerzőkollektíva Kdo H II 1 (2), 2017
- 13 Maaßen, egy, a szerzőhöz intézett e-mailjében, 2018
- 14 Sanger, 2018, 279.
- 15 Coats, Worldwide Threat Assessment of The Intelligence Community, 2019
- 16 Office of the Secretary of Defense, 2018, VII. o.
- 17 Barbes, 2018
- 18 Ischinger, Interjú Wolfgang Ischingerrel, 2018, 31. hivatk.
- 19 Koch & Riedel, 2018
- 20 Vestner, 2018, 39. hivatk.
- 21 A *Süddeutsche Zeitung* gazdasági csúcsán, 2013. nov. 13., Berlin, a „keresztkérdések” során
- 22 Chomsky, 2016, 15. o.
- 23 University of Cambridge; DROG, dátum nélkül
- 24 Scola & Gold, 2018
- 25 Stanton, 2019

- 26 Chesney, 2018
- 27 L. még ezzel kapcsolatban Menzel számos példáját in: Die Ordnung der Welt, 2015
- 28 Horowitz, Allen, Kania, & Scharre, 2018, 8. o.
- 29 Bundesregierung, 2018, 1. o.
- 30 Koch W., egy a szerzőnek írt e-mail-jében, 2018

[ZÁRSZÓ]

Amikor az igény találkozik a valósággal

- 1 Department of Defense, 2019
- 2 Lockie, 2109
- 3 Reid, 2019

Bibliográfia

A szerző által készített interjúk itt olvashatók: <https://www.yvonnehofstetter.de/der-unsichtbare-krieg/interviews/>

AFP news agency (2018. augusztus 4.): „Footage shows moment of explosion during Maduro’s speech”, letöltve innen, 2018. október 24-én: *Youtube*: https://www.youtube.com/watch?v=tI0Hrz9FqJk&feature=player_embedded

Allan, I. (2018. június 13.): „US imposes sanctions on companies for helping Russian spy agencies”, letöltve innen, 2018. július 27-én: *intelNews*: <https://intelnews.org/2018/06/13/01-2338/>

Allan, J. (nyug.) tábornok, Breedlove P. (nyug.) tábornok, Lindley-French, J. & Zambellas, G. (nyug.) admirális. (2017): *Future War NATO? From Hybrid War to Hyper War via Cyber War*. Bratislava: Globsec.

Anonym (2018. szeptember 5.): „I Am Part of the Resistance Inside the Trump Administration”, letöltve innen, 2019. január 15-én: *The New York Times*, https://www.nytimes.com/2018/09/05/opinion/trump-white-house-anonymousresistance.html?utm_source=newsletter&utm_medium=

um= email&utm_campaign=sendto_newsletter&stream=top

Arendt, H. (2015): *Elemente und Ursprünge totaler Herrschaft*. 18. kiad. München/Berlin: Piper. (Magyarul: *A totalitarizmus gyökerei*. Budapest: Európa Könyvkiadó, 1992)

Arendt, H. (1969): *On Violence*. Cheshire: Stellar Classics.

Arendt, H. (1972): *Wahrheit und Lüge in der Politik*. Zwei Essays. München/Berlin: Piper.

Arendt, H. (2018): *Die Freiheit, frei zu sein*. München: dtv.

Azzellini, D. (2006. március 3.): „Wie Söldner zu Geschäftleuten wurden”, letöltve innen, 2018. június 13-án: Heise: [https://www.heise.de: https://www.heise.de/tp/features/Wie-Soeldner-zu-Geschaeftleuten-wurden-3405196.html](https://www.heise.de/tp/features/Wie-Soeldner-zu-Geschaeftleuten-wurden-3405196.html)

Backes, T., Jaschensky, W., Langhans, K., Munzinger, H., Witzemberger, B. & Wormer, V. (2016. szeptember 30.): „Timeline der Panik”, letöltve innen, 2018. augusztus 15-én: *Süddeutsche Zeitung*: <https://gfx.sueddeutsche.de/apps/57eba578910a46f716ca829d/www/>

Barber, L., Sevastopulo, D. & Tett, G. (2017. április 2.): „Donald Trump: Without Twitter, I would not be here – FT interview”, letöltve innen, 2008. augusztus 19-én: *Financial Times*: <https://www.ft.com/content/943e322a-178a-11e7-9c35-0dd2cb31823a>

Barnes, J. (2018. október 28.): „U.S. Begins First Cyberoperation Against Russia Aimed at Protecting Elections”, letöltve innen, 2019. január 30-án: *The New York Times*: <https://www.nytimes.com/2018/10/28/us/politics/us-cyber-operation-against-russia.html>

[ps://www.nytimes.com/2018/10/23/us/politics/russian-hacking-usa-cyber-command.html?smtyp=cur&smid=tw-nytimes](https://www.nytimes.com/2018/10/23/us/politics/russian-hacking-usa-cyber-command.html?smtyp=cur&smid=tw-nytimes)

BBC News (2017. május 17.): „Massive ransomware infection hits computers in 99 countries”, letöltve innen, 218. május 28-án: *BBC*: <http://www.bbc.com/news/technology-39901382>

Becker-Wenzel, A. & Beuscher, M. (2018. szeptember 4.): „Kulturzeit”, letöltve innen, 2018. szeptember 10-én innen: *3sat Kulturzeit*: <http://www.3sat.de/mediathek/?mode=play&obj=75552>

Bidder, B. (2017 június 5.): „Darum geht es beim Konflikt am Golf”, letöltve innen, 2018. augusztus 18-án: *Manager Magazin*: <http://www.manager-magazin.de/politik/welt-wirtschaft/katar-die-hintergruende-des-konflikts-mit-saudi-arabien-a-1150743.html>

Biermann, K. & Wiegold, T. (2015): *Drohnen. Chancen und Gefahren einer neuen Technik*, Bonn: Bundeszentrale für politische Bildung.

Bing, C. (2018. december 6.): „Exclusive: Clues in Marriott hack implicate China-sources”, letöltve innen, 2019. február 14-én: *Thomson Reuters*: <https://uk.reuters.com/article/uk-marriott-intnl-cyber-china/clues-in-marriott-hack-implicate-china-sources-idUKKBN1O504B>

Bob, Y. J. (2018. június 18.): „Ex-‘Israeli NSA’ chief: Target Iran, Hezbollah energy infrastructure first”, letöltve innen, 2018. július 26-án: *The Jerusalem Post*: <https://www.jpost.com/Is->

rael-News/Ex-Israeli-NSA-chief-Target-Iran-Hezbollah-energy-infrastructure-first-560210

Borchert, H. (2018. március 4.): Interjú Heiko Borcherttel. (Készítette Y. Hofstetter)

Bossert, T. P. (2017. december 18.): „It’s Official: North Korea Is Behind WannaCry”, letöltve innen, 2018. június 24-én: *Wall Street Journal*: https://www.wsj.com/articles/its-official-north-korea-is-behind-wannacry-1513642537#comments_sector

Boyd, A. (2018. október 31.): „Pentagon Doesn’t Want Real Artificial Intelligence In War, Former Official Says”, letöltve innen, 2018. november 2-án: *Defense One*: https://www.defenseone.com/technology/2018/10/pentagon-doesnt-want-real-artificial-intelligence-war-former-official-says/152450/?oref=d_brief_nl

Brennan, J. (2017. július 27.): „The Putin Files: John Brennan (2013–2017). Putins Revenge II”, letöltve innen, 2018. június 20-án: *Public Broadcasting Service*: <https://www.pbs.org/wgbh/frontline/interview/john-brennan/>

Browder, B. (2016): *Red Notice: Wie ich Putins Staatsfeind Nr. 1 wurde*. München: dtv.

Bundesakademie für Sicherheitspolitik, Auswärtiges Amt & Heinrich-Böll-Stiftung (2019): *Künstliche Intelligenz und Autonomie – Autonome und halbautonome Waffensysteme als Herausforderung für die Sicherheitspolitik*. Berlin: Bundesakademie für Sicherheitspolitik; Auswärtiges Amt; Heinrich-Böll-Stiftung.

- Bundesamt für Verfassungsschutz (2018): Cyber-Brief Nr. 01/2018. Berlin/Köln: Bundesamt für Verfassungsschutz.
- Bundesregierung (2018): Eckpunkte der Bundesregierung für eine Strategie Künstliche Intelligenz. Berlin: Bundesregierung.
- Calabresi, M. (2018): „The Secret History of an Election”, in: *Special Time Edition*, New York, NY: Time Inc. Books, 34–41.
- Calamur, K. (2017. július 17.): „Who Hacked Qatar’s News Sites?”, letöltve innen, 2018. augusztus 8-án: *The Atlantic*: <https://www.theatlantic.com/news/archive/2017/07/uae-denies-qatar-hack-charges/533826/>
- Campaign to Stop Killer Robots (2018. április 13.): „Convergence on retaining human control of weapons systems”, letöltve innen, 2018. október 31-én: *stopkillerrobots.org*: https://www.stopkillerrobots.org/wp-content/uploads/2018/04/KRC_CountryViews_13Apr2018.pdf
- Carlin, J. (2018. július 16.): „Putin Is Running a Destructive Cybercrime Syndicate Out of Russia, letöltve innen, 2019. január 2-án: *The New York Times*: https://www.nytimes.com/2018/07/16/opinion/trump-putin-russia-cybercrime.html?mkt_tok=eyJpIjoiTVdRNFkyWTNZV0ppWldFMCIIsInQiOiJOaWJNMjVvTnlwQlkzMjVVRVXlobk9yWD-RUNWtcL0ZyU2FOWTZDbmZmQ0M5dDdTNXFzcGVqTz-ByUG9pc1dUT0RVU0k5b1ZcL0FcL1NGbkhmTUdX-cE5mVjZuQkdSTUdBZ05vT
- Carvin, S. & Williams, M. (2015): *Law, Science and Liberalism and the American Way of Warfare*. Cambridge: Cambridge

University Press.

CDU, CSU & SPD (2018. február 7.): „Koalitionsvertrag zwischen CDU, CSU und SPD”, letöltve innen, 2018. október 31-én: *Die Bundesregierung*: <https://www.bundesregierung.de/bregde/themen/koalitionsvertrag-zwischen-cdu-csu-und-spd-195906>

Central Intelligence Agency (2019. február 28.): „CIA World Factbook”, letöltve innen, 2019. március 5-én: *Central Intelligence Agency*: <https://www.cia.gov/library/publications/resources/the-world-factbook/geos/rs.html>

Chesney, R. (2018. október 17.): „How Realistic Fake Video Threatens Democracies”, letöltve innen, 2019. február 8-án: *Defense One*: <https://www.defenseone.com/threats/2018/10/how-deep-fakes-threaten-democracies/152093/>

Chomsky, N. (2016): *Profit Over People. War Against People*. 8. kiad. München/Berlin: Piper Verlag.

CNN Wire Staff (2011. szeptember 29.): „Man, 26, charged in plot to bomb Pentagon using model airplane”, letöltve innen, 2018. október 24-én: *CNN*: <https://edition.cnn.com/2011/09/28/us/massachusetts-pentagon-plot-arrest/>

Coats, D. (2018. július 13.): *Dialogues on American Foreign Policy and World Affairs: Director of National Intelligence Dan Coats and Walter Russell Mead*, Washington, D.C.: Hudson Institut; letöltve innen, 2018. július 27-én: <https://www.hudson.org/research/14456-full-transcript-dialogues-on-american-foreign-policy-and-world-affairs-director-of-national-intelligence-dan-coats-and-walter-russell-mead>

Coats, D. (2019. január 29.): „Worldwide Threat Assessment of The Intelligence Community”, letöltve innen, 2019. január 27-én: *US Senate Select Committee on Intelligence*: <https://www.intelligence.senate.gov/sites/default/files/documents/os-dcoats-012919.pdf>

Coldewey, D. & Hatmaker, T. (2017. november 11.): „Here are the Russian ads that deceived users on Facebook and Instagram, letöltve innen, 2018. szeptember 26-án: *TechCrunch*: <https://techcrunch.com/gallery/here-are-15-of-the-russian-boughtads-aimed-at-influencing-the-election/slide/9/>

Das, K., & Spicer, J. (2016. július 21.): „How the New York Fed fumbled over the Bangladesh Bank cyber-heist”, letöltve innen, 2019. február 15-én: *Thomson Reuters*: <https://www.reuters.com/investigates/special-report/cyber-heist-federal/>

Defense One Radio (2018. szeptember 21.): „Episode 21: How to Kill a Drone”, letöltve innen, 2018. november 10-én: *Defense One Radio*: <https://www.defenseone.com/ideas/2018/09/ep-21-how-kill-drone-toward-smarter-cheaper-us-presence-middleeast-and-more/151468/?oref=d-channelriver>

DeGeurin, M. (2018. július 13.): „Russia’s Alternate Internet”, letöltve innen, 2018. augusztus 9-én: *SelectAll by New York Media*: http://nymag.com/selectall/2018/07/russia-dns-alternative-internet-could-yield-cyberattack.html?mkt_tok=eyJpIjoiTVdRNFkyWTNZV0ppWldFMCIzInQiOiJ0aWJNMfVv-TnlwQlkzMfVRVXlobk9yWDRUNWtcL0ZyU2-FOWTZDbmZmQ0M5dDdTNXFzcGVqTzByUG9pc1dUT0R-VU0k5b1ZcL0FcL1NGbkhmTUdXcE5

- Department of Defense (2012. november 21.): „Directive 3000.9”, letöltve innen, 2018 október 30-án: *Executive Services Directorate*: www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/300009p.pdf
- Department of Defense (2019. február 12.): „Summary of the 2018 Department of Defense Artificial Intelligence Strategy: Harnessing AI to Advance Our Security and Prosperity”, letöltve innen, 2019. február 13-án: *media.defense.gov*: <https://media.defense.gov/2019/Feb/12/2002088963/-1/-1/1/SUMMARY-OF-DOD-AI-STRATEGY.PDF>
- Dillet, R. (2018. július 26.): „Facebook officially loses \$123 billion in value”, letöltve innen, 2018. július 26-án: *TechCrunch*: https://techcrunch.com/2018/07/26/facebook-officially-loses-123-billion-in-value/?utm_medium=TCnewsletter
- Dörr, D. & Natt, A. (2014): „Suchmaschinen und Meinungsvielfalt – Ein Beitrag zum Einfluss von Suchmaschinen auf die demokratische Willensbildung”, in: *ZUM-Zeitschrift für Urheber- und Medienrecht*. Baden-Baden: Nomos, 829-853.
- Dörr, O. (2004. október 15.): „Gewalt und Gewaltverbot im modernen Völkerrecht”, letöltve innen, 2018. december 6-án: *Bundeszentrale für politische Bildung*: <http://www.bpb.de/apuz/28036/gewalt-und-gewaltverbot-im-modernen-voelkerrecht?p=all>
- Drevstad, C. (2012. szeptember 27.): „TAURUS KEPD 350. The Modular Stand Stand-off Missile for Precision Strike against HDBT”, letöltve innen, 2018. október 30-án: *Wikimedia Tool-*

forge: https://tools.wmflabs.org/giftbot/deref.fcgi?url=http%3A%2F%2Fwww.dtic.mil%2Fndia%2F2008p-sa_apr%2Fdrevstad.pdf

Eberlein, S. [rendező] (2018): Stadt in Angst [mozifilm]. München: ARD; letöltve innen, 2018. augusztus 15-én ARD: <https://www.ardmediathek.de/tv/DoX-Der-Dokumentarfilm-im-BR/M%C3%BCnchen-Stadt-in-Angst/BR-Fernsehen/Video?bcastId=24831852&documentId=54155602>

Eichmeier, R. (2018): „Maschinerie der NS-Propaganda Lug im ‘Dritten Reich’”. München: Bayerischer Rundfunk, BR2 radioWissen; letöltve innen, 2018. augusztus 20-án: BR: <https://www.br.de/mediathek/podcast/radiowissen/ns-propagandamaschinerie-lug-im-dritten-reich/1029719>

Emmott, R., & Wroughton, L. (2018. július 8.): „Transatlantic ties hang in the balance as Trump comes to Europe”, letöltve innen, 2018. július 11-én: *Reuters*: https://www.reuters.com/article/us-usa-trump-europe/transatlantic-ties-hang-in-the-balance-as-trump-comes-to-europe-idUS-KBN1JY059?mkt_tok=eyJpIjoiTURFd01XTmpNak13Tm1Sa-CIsInQiOiJOTGRKQ3NuV2lZdkVBSmd2Rk5Td01sV2VTe-UZ4OUZDM0wrdlFcL242dEtQRGhOVWMzcCtlSHhqRHVMe

Federal Aviation Association (2016. március 24): „FAA Releases 2016 to 2036 Aerospace Forecast”, letöltve innen, 2018. október 24-én: *FAA*: <https://www.faa.gov/news/updates/?newsId=85227>

Fehér Ház (2018. július 16.): „Remarks by President Trump and President Putin of the Russian Federation in Joint Press

Conference”, letöltve innen, 2018. augusztus 20-én: *White-house*: <https://www.whitehouse.gov/briefings-statements/remarks-president-trump-president-putin-russian-federation-joint-press-conference/>

Feinberg, A. (2018. január 11.): „Exclusive: Here Is A Draft Of Trump’s Nuclear Review. He Wants A Lot More Nukes”, letöltve innen, 2018. július 28-án: *Huffington Post*: https://www.huffingtonpost.com/entry/trump-nuclear-posture-review-2018_us_5a4d4773e4b06d1621bce4c5

Ferguson, N. (2018): *Türme und Plätze*. Berlin: Propyläen.

Foltz, A. C. (2012): „Stuxnet, Schmitt Analysis, and the Cyber ‘Use-of-Force’ Debate”, letöltve innen, 2018. december 6-án: *National Defense University Press*: http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-67/JFQ-67_40-48_-Foltz.pdf

Fredericks, B. (2018. július 28.): „Trump will campaign ‘6 or 7’ days a week for GOP candidates”, letöltve innen, 2018. augusztus 20-án: *New York Post*: <https://nypost.com/2018/07/27/trump-will-campaign-6-or-7-days-a-week-for-gop-candidates/>

G20 (2017. március 17–18.): „G20 Finance Ministers and Central Bank Governors Meeting – Communiqué”, letöltve innen, 2018. július 27-én: *Carnegie Endowment*: <http://carnegieendowment.org/files/g20-communicue.pdf>

Gabriel, M. (2015): *Ich ist nicht Gehirn*. Berlin: Ullstein.

Gabriel, M. (2018): *Der Sinn des Denkens*. Berlin: Ullstein.

- Gabriel, S. (2018. február 17): „Rede von Außenminister Sigmar Gabriel bei der Münchner Sicherheitskonferenz”, letöltve innen, 2018. június 8-án: *Auswärtiges Amt*: <https://www.auswaertiges-amt.de/de/newsroom/rede-muenchner-sicherheitskonferenz/1599848>
- Galeotti, M. (2014. szeptember 12.): „Wie weit wird er gehen?”, letöltve innen, 2019. február 14-én: *The European*: <https://www.theeuropean.de/mark-galeotti--3/8984-putinstaktik-gegen-den-westen>
- Garamone, J. (2018. június 26.): „Defense Intelligence Agency Bringing Forewarning into 21st Century”, 2018. augusztus 19-én: *U.S. Department of Defense*: <https://www.defense.gov/News/Article/Article/1560813/defense-intelligence-agency-bringing-forewarning-into-21st-century/>
- Geiß, R. (2014): „Lethal Autonomous Weapon Systems. Technology, Definition, Ethics, Law & Security”, in: *Lethal Autonomous Weapon Systems. Technology, Definition, Ethics, Law and Security*. Berlin: Federal Foreign Office, 2–4.
- Geiß, R. (2015. június): „Die völkerrechtliche Dimension autonomer Waffensysteme”, letöltve innen, 2018. október 5-én: *Friedrich Ebert Stiftung*: library.fes.de/pdf-files/id/ipa/11444-20150619.pdf
- Gerasimov, V. (2013. február 27.): „The Value of Science in Prediction”, in: *Military-Industrial Kurier*, Nr. 8 (476), 2–3.; letöltve innen, 2018. június 6-án: http://vpk-news.ru/sites/default/files/pdf/VPK_08_476.pdf

Giacca, G. (2014): „Legal Review of New Weapons, Means and Methods of Warfare”, in: *Lethal Autonomous Weapon Systems. Technology, Definition, Ethics, Law and Security*, Berlin: Federal Foreign Office, 119-127.

Google Books Ngram Viewer (2018. szeptember 24.): „subversion, subversive”, letöltve innen, 2018. szeptember 24-én *Google Books Ngram Viewer*: https://books.google.com/ngrams/graph?content=subversion%2Csubversive&case_insensitive=on&year_start=1800&year_end=2008&corpus=20&smoothing=3&share=&direct_url=t4%3B%2Csubversion%3B%2Cc0%3B%2Cs0%3B%3BSubversion%3B%2Cc0%3B%3Bsubversion%3B%2Cc0%3B.t4%3B%2Cs

Gray, C. S. (2015): *The Future of Strategy*. Malden, MA: Polity Press.

Guardian staff and agencies (2018. július 19.): „‘Very aggressive’: Trump suggests Montenegro could cause world war three”, letöltve innen, 2018. július 28-án: *The Guardian*: <https://www.theguardian.com/us-news/2018/jul/19/very-aggressive-trump-suggests-montenegro-could-cause-world-war-three>

Hamilton, A. (1787. október 17.): „The Federalist Papers. The Federalist 1”, letöltve innen, 2018 augusztus 27-én: *American History*: <http://www.let.rug.nl/usa/documents/1786-1800/the-federalist-papers/the-federalist-1.php>

Harari, Y. N. (2017): *Homo Deus*. München: C. H. Beck.

- Hayden, M. V. (2018): *The Assault on Intelligence. American National Security in an Age of Lies*. New York, NY: Penguin Press.
- Hellestveit, C. (2014): „Accountability for Lethal Autonomous Weapon Systems under International Humanitarian Law”, in: *Lethal Autonomous Weapon Systems. Technology, Definition, Ethics, Law and Security* Berlin: Federal Foreign Office, 135–147.
- Hofstetter, Y. (2016): *Das Ende der Demokratie*. München: C. Bertelsmann.
- Horn, E. (2008. szeptember): „Schweigen, Lügen, Schwätzen. Eine kurze Geschichte der politischen Unwahrheit”, szerk. U. van Loyen & M. Neumann, in: *Tumult Nr. 34: Unter uns – Strategien der Diskretion*, 112–122.; letöltve innen, 2018. augusztus 29-én: https://germanistik.univie.ac.at/fileadmin/user_upload/inst_germanistik/Wiss_Arbeiten/Horn/Schweigen__L%C3%BCgen__Schw%C3%A4tzen.pdf
- Horowitz, M. C., Allen, G. C., Kania, E. B. & Scharre, P. (2018): „Strategic Competition in an Era of Artificial Intelligence”, letöltve innen, 2018. augusztus 4-én: *Center For A New American Security*: <https://www.cnas.org/publications/reports/strategic-competition-in-an-era-of-artificial-intelligence>
- Horseman, J. (2016. július 8.): „Claims of tampering with state’s online voter registration”, letöltve innen, 2018. június 20-án *Record Bee Community News*: <http://www.record-bee.com/article/NQ/20160708/NEWS/160709894>

- Inglehart, R. F., & Norris, P. (2016. augusztus): *Trump, Brexit, and the Rise of Populism*. Cambridge, MA: Harvard Kennedy School.
- Inozemtsev, V. (2018. március–április): „Der russische Kreisel”, in: *Internationale Politik*, 2. sz., 73. évf., 50–57.
- International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence (2017): *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press.
- International Monetary Fund (2018. október): „Inflation rate, average consumer prices”, letöltve innen, 2018. október 24-én: IMF: <https://www.imf.org/external/datamapper/PC-PIPCH@WEO/WEOWORLD/VEN>
- Ischinger, W. (2017. december 12.): Előadás a Bayerischer Hofban, München: Zukunftsfragen deutscher und europäischer Sicherheitspolitik.
- Ischinger, W. (2018. május 22.): Interjú Wolfgang Ischingerrel (készítette Y. Hofstetter).
- Ischinger, W. (2018): *Welt in Gefahr*. Berlin: Econ.
- Kalmanovitz, P. (2014): „Lethal Autonomous Weapon Systems and the Risk of ‘Riskless Warfare’”, in: *Lethal Autonomous Weapon Systems. Technology, Definition, Ethics, Law and Security*, Berlin: Federal Foreign Office, 184–195.
- Kilcullen, D. (2015): *Out of The Mountains. The Coming Age of The Urban Guerilla*. London: C. Hurst & Co. (Publishers) Ltd.

Kínai Kommunista Párt Központi Bizottsága (2013. november 8.): „Document 9: A ChinaFile Translation”, letöltve innen, 2018. december 26-án: *Chinafile*: <http://www.chinafile.com/document-9-chinafile-translation>

Kissinger, H. (2018. május 15.): „How the Enlightenment Ends”, letöltve innen, 2018. szeptember 5-én: *The Atlantic*: <https://www.theatlantic.com/magazine/archive/2018/06/henry-kissinger-ai-could-mean-the-end-of-human-history/559124/>

Kobek, J. (2016): *Ich hasse dieses Internet*. Frankfurt am Main: S. Fischer.

Koch, M., & Riedel, D. (2018. június 6.): „Germany could dispatch armed forces in response to cyberattacks”, letöltve innen, 2019. január 31-én: *Handelsblatt*: https://www.handelsblatt.com/today/politics/hekker-soldiers-germany-could-dispatch-armed-forces-in-response-to-cyberattacks/23582348.html?mkt_tok=eyJpIjoiWm1JMTkySXh-PV0UwWlRKaSIsInQiOiJxNkwzekcwSWxCeGVKS0hcL2Z-wOUZKR21ZWdDgxZWdRaE9vdWRUTEtZV09sMHPsdl-rOGFKM

Koch, W. (2018. augusztus 30.). E-mail a szerzőnek.

Koch, W. (2018): *Künstliche Intelligenz? Die Algorithmenwelt und menschliche Verantwortung*. Bonn: Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie FKIE.

Koch, W. (2018. szeptember 5.): *On Detecting Radiological Bombs With Potential Applications to Field Camp and Soldier Pro-*

tection. Bonn: Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie FKIE.

Koch, W. (2019): *Menschliche Verantwortung als Leitgedanke für technisches Design bei FCAS. Draft V0.3*. Bonn: Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie FKIE.

Kovacs, E. (2018. február 3.): „U.S., Canada, Australia Attribute NotPetya Attack to Russia”, letöltve innen, 2018. július 26-án: *Securityweek*: <https://www.securityweek.com/us-canada-australia-attribute-notpetya-attack-russia>

Langner, A. (1969): „Philosophie und Politik bei Karl Jaspers”, in: *Jahrbuch für Christliche Sozialwissenschaften*, CSW 10 (1969), 273–299.; letöltve innen, 2018. augusztus 29-én: <https://www.uni-muenster.de/Ejournals/index.php/jcsw/article/view/900/847>

Lepault, S. & Franklin, R. (2018. december 18.): Die Welt des Xi Jinping, letöltve innen, 2018. december 26-án: *ARTE*: <https://www.arte.tv/de/videos/078193-000-A/diewelt-des-xi-jinping/>

Lobe, A. (2018. július 31.): „Die Gesellschaft der Metadaten”, letöltve innen, 2018. augusztus 19-én: *Süddeutsche Zeitung*: <https://www.sueddeutsche.de/digital/philosophie-die-gesellschaft-der-metadaten-1.4070474>

Lockie, A. (2019. január 11.): „China sets the stage for a ‘bloody nose’ attack on US aircraft carriers, but it would backfire horribly”, letöltve innen, 2019 február 12-én: *Business Insider Deutschland*: <https://www.businessinsider.de/chinas-th->

reats-to-attack-us-aircraft-carriers-would-backfire-horribly-2019-1?r=US&IR=T

Luhman, N. (1994). Interjú, letöltve innen, 2018. június 10-én:

Fifo Ost: <http://www.fifoost.org/?p=904>

Maaßen, H.-G. (2018. május 14-én). Interjú Hans-Georg-Maaßen-nel (készítette Y. Hofstetter).

Maaßen, H.-G. (21. Dezember 2018). E-mail a szerzőnek.

Mansholt, M. (2018. február 28.): „APT28 – das sind die Hekker hinter dem Angriff auf das Bundesnetzwerk”, letöltve innen, 2018. július 27-én: *Stern*: <https://www.stern.de/digital/online/apt28---das-sind-die-hekker-hinter-dem-angriff-auf-das-bundesnetzwerk-7881400.html>

Martínez, A. G. (2016): *Chaos Monkeys. Obscene Fortune and Random Failure in Silicon Valley*. New York, N.Y.: HarperCollins.

Maurer, T. (2018): *Cyber Mercenaries*. Cambridge: Cambridge University Press.

Maurer, T., Levite, A. & Perkovich, G. (2017. március 27.): „Toward a Global Norm Against Manipulating the Integrity of Financial Data”, letöltve innen, 2018. július 27-én: *Carnegie Endowment for International Peace*: <http://carnegieendowment.org/2017/03/27/toward-global-norm-against-manipulating-integrity-of-financial-data-pub-68403> Mayer-Kuckuk, F. (2018. július–augusztus): „KI für Xi”, in: *Internationale Politik*, 4. sz., 73. évf., 36-39.

McKinsey&Company (dátum nélkül): „Real-World AI”, letöltve innen, 2018. október 5-én: *McKinsey&Company*: <https://www.mckinsey.com/featured-insights/artificial-intelligence/five-fifty-real-world-ai?cid=other-eml-alt-mkq-mck-oth-1806&hlkid=ea15729fca644854ab83bee7b1-ce84aa&hctky=9214885&hdpid=c6a15a76-825b-42e9-ae81-731a83b89db5> McLuhan.

McLuhan, H. M. (1970): *Culture is our Business*. Eugene, OR: Wipf and Stock.

Meadows, D. (2017. szeptember 12.): Presentation to the Club of Vienna.

Menzel, U. (2015): *Die Ordnung der Welt*. Berlin: Suhrkamp.

Menzel, U. (2018. március 7.). Interjú Ulrich Menzellel (készítette Y. Hofstetter).

Menzel, U. (2018. június): „Die neue eurasische Weltordnung”, in: *Blätter für deutsche und internationale Politik*, 6/18, 49–60.

Mills, C. W. (1956): *The Power Elite*. Oxford: Oxford University Press.

Ministry of Defence (2018): *Joint Concept Note 1/18: Human-Machine Teaming*. London: Ministry of Defence.

Mortensen, D. R. (2017. június 20.): „Using AI to program humans to behave better”, letöltve innen, 2017. december 26-án: *LinkedIn*: https://www.linkedin.com/pulse/using-ai-program-humans-behave-better-dennis-r-mortensen/?trk=eml-email_feed_ecosystem_digest_01-hero-0-null&midTo-

ken=AQE2Xrxn6jNXEw&fromEmail=fromEmail&ut=3xzMM1-m4Hl8g1

Münkler, H. (2004): *Die neuen Kriege*. Berlin: Rowohlt.

Münkler, H. (2015): „Hybrid Wars. The Dissolution of the Binary Order of War and Peace, and Its Consequences”, in: *Ethics and Armed Forces*, 2. sz., 20–23.; letöltve innen, 2018. november 24-én: http://www.ethikundmilitaer.de/fileadmin/inhalt-medizinethik/Hybrid_Warfare-Enemies_at_a_Loss_2015-2.pdf

NASA (2014. június 11.): „Sun Emits 3 X-class Flares in 2 Days”, letöltve innen, 2018. november 10-én: NASA: <https://www.nasa.gov/content/goddard/sun-emits-3-x-classflares-in-2-days/>

NATO (2014. szeptember 5.): „Wales Summit Declaration”, letöltve innen, 2018. november 10-én: NATO: https://www.nato.int/cps/en/natohq/official_texts_112964.htm
Newman, N., Fletcher, R., Kalogeropoulos, A., Levy, D. A. & Nielsen, R. K. (2018): *Reuters Institute Digital News Report 2018*. Oxford: University of Oxford; Reuters Institute for the Study of Journalism; letöltve innen, 2018. szeptember 9-én: <http://media.digitalnewsreport.org/wp-content/uploads/2018/06/digital-news-report-2018.pdf?x89475>

Nichols, T. M. (2017): *The Death of Expertise*. New York, N.Y.: Oxford University Press.

Nolte, G. (2018): „Recht in Kriegen – Herfried Münkler als Herausforderung”, in: G. Straßenberger, & F. Wassermann (szerk.), *Staatserzählungen*, Berlin: Rowohlt, 110–126.

- Office of the Director of National Intelligence (2017. január 6.): „Background to ‘Assessing Russian Activities and Intentions in Recent US Elections’: The Analytic Process and Cyber Incident Attribution”, letöltve innen, 2018. szeptember 22-én: *Office of the Director of National Intelligence*: https://www.dni.gov/files/documents/ICA_2017_01.pdf
- Office of the Secretary of Defense (2018. február): „Nuclear Posture Review”, letöltve innen, 2018. november 24-én: *U.S. Department of Defense*: <https://dod.defense.gov/News/Special-Reports/2018NuclearPostureReview.aspx>
- Panetta, L. E. (2012. október 11.): „Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security”, letöltve innen, 2018. november 20-án: *U.S. Department of Defense*: <http://archive.defense.gov/transcripts/transcript.aspx?transcriptid=5136>
- Paquette, E. (2015. június 9.): „Piratage de TV5 Monde: l’enquête s’oriente vers la piste russe”, letöltve innen, 2018. június 27-én: *L’Express*: https://www.lexpress.fr/actualite/medias/piratage-de-tv5-monde-la-piste-russe_1687673.html
- Patrikarakos, D. (2017): *War in 140 Characters*. New York, NY: Basic Books.
- Pearson, R. (2017): *Advanced Technologies for Collective Defence within NATO*. Wimborne Minster, Dorset: Cobham plc.
- Perkins, J. (2016): *Bekenntnisse eines Economic Hit Man. Unterwegs im Dienst der Wirtschaftsmafia*. München: Goldmann.

- Polizei Bayern (2017. március 17.): „Ermittlungen zum Münchner Amoklauf abgeschlossen”, letöltve innen, 2018. augusztus 27-én: *Polizei Bayern Landeskriminalamt*: <http://archive.is/wiHMz#selection-1149.0-1149.48>
- Pompeo, M. (2018. december 4.): „Restoring the Role of the Nation-State in the Liberal International Order”, letöltve innen, 2019. március 5-én: *US Department of State*: <https://www.state.gov/secretary/remarks/2018/12/287770.htm>
- Prisching, M. (2017): „Soziologie der kollektiven Ängste”, in: *Theologisch-praktische Quartalsschrift* (4), Regensburg: Verlag Friedrich Pustet, 339–347.
- Prose, F. (2015. május 15.): „Writing From a War Zone Doesn’t Make You Anne Frank”, letöltve innen, 2018. augusztus 18-án: *Foreign Policy*: <https://foreignpolicy.com/2015/05/15/writing-from-a-war-zone-doesnt-make-you-anne-frank-girl-emulated-farah-baker-zlata-filipovic/>
- Reid, D. (2019. február 11.): „UK to send new aircraft carrier loaded with F35 jets into South China Sea”, letöltve innen, 2019. február 12-én: *CNBC.com*: <https://www.cnbc.com/2019/02/11/uk-to-send-new-aircraft-carrier-loaded-with-f35-jets-into-south-china-sea.html>
- Rickli, J.-M. (2018. márc. 24). Interjú Jean-Marc Ricklivel (készítette Y. Hofstetter).
- Rickli, J.-M., & Krieg, A. (2018): „Surrogate warfare: the art of war in the 21st century?”, in: *Defence Studies*, 18/2, 113-130. doi:10.1080/14702436.2018.1429218

Rid, T. (2018): *Mythos Cyberwar – Über digitale Spionage, Sabotage oder andere Gefahren*. Hamburg: Edition Körber.

Ries, T., Bersoff, D., Armstrong, C., Adkins, S. & Bruening, J. (2018): „2018 Edelman Trust Barometer: Global Report”, letöltve innen, 2018. szeptember 28-án: *Edelman*: <https://www.edelman.com/trust-barometer>

Roosevelt, T. (1924):, 14 köt., a T. R. Association kiadása, New York: Charles Scribner's Sons; letöltve innen, 2018. szeptember 22-én: www.theodore-roosevelt.com/images/research/worksoftheodoreroosevelt/TRMEMORIAL-WORKS14.pdf

Sainato, M. (2016. július 14.): „California Calls Fraud: Demands DNC Investigation”, letöltve innen, 2018. június 19-én: *Observer*: <http://observer.com/2016/07/california-calls-fraud-demands-dnc-investigation/>

Salisbury, P. (2017. október 20.): „The fake-news hack that nearly started a war this summer was designed for one man: Donald Trump”, letöltve innen, 2018. augusztus 8-án: *Quartz*: <https://qz.com/1107023/the-inside-story-of-the-hack-that-nearly-startedanother-middle-east-war/>

Sanger, D. (2018): *The Perfect Weapon*. London: Scribe.

Sauer, F. (2018): *Künstliche Intelligenz in den Streitkräften: Zum Handlungsbedarf bei Autonomie in Waffensystemen*. Arbeitspapier Sicherheitspolitik, Nr. 26, Berlin: Bundesakademie für Sicherheitspolitik.

- Schäffle, A. (1897): „Über den wissenschaftlichen Begriff der Politik”, szerk. A. Schäffle, in: *Zeitschrift für die gesamte Staatswissenschaft*, 53 (4), 579–600; letöltve innen, 2018. június 12-én: <https://www.digizeitschriften.de/dms/img/?PID=GDZPPN001726501&physid=phys615#navi>
- Schmidt, M. S. (2018. július 13.): „Trump Invited the Russians to Hack Clinton. Were They Listening?”, letöltve innen, 2018. július 25-én: *The New York Times*: <https://www.nytimes.com/2018/07/13/us/politics/trump-russia-clinton-emails.html>
- Scholz, R. (2018. október 16.). A szerzőhöz intézett e-mailjéből.
- Scola, N., & Gold, A. (2018. szept 4.): „Twitter says Trump not immune from getting kicked off”, letöltve innen, 2019. február 8-án: *Politico*: <https://www.politico.eu/article/donald-trump-twitter-not-immune-from-getting-kicked-off/>
- Scott, C. P. (1921): *History of the Guardian and The Observer*. Manchester: Guardian.
- Sepulvado, J. (2017. július 12.): „DA: Hekkers Penetrated Voter Registrations in 2016 Through State’s Election Site”, letöltve innen, 2018. június 19-én: *KQED*: <https://www.kqed.org/news/11579541/hekkers-penetrated-voter-registrations-in-2016-through-states-election-site>
- Siegele, L. (2018. július-augusztus): „Eine Frage der Zeit”, in: *Internationale Politik*, 4. sz, 73. évf., 8-13.
- Silver, A. (2018. november 30.): „China set to launch first-ever spacecraft to the far side of the Moon”, letöltve innen, 2019

január 5-én: *Nature*: <https://www.nature.com/articles/d41586-018-07562-z>

Simms, B. & Laderman, C. (2017): *Wir hätten gewarnt sein können: Donald Trumps Sicht auf die Welt*. Bonn/München: Deutsche Verlags-Anstalt.

Singer, P. W. & Brooking, E. T. (2018): *LikeWar: The Weaponization of Social Media*. Boston MA: Houghton Mifflin Harcourt.

Smith, B. (2017. máj. 14.): „The need for urgent collective action to keep people safe online: Lessons from last week’s cyberattack”, letöltve innen, 2108. május 28-án: *Microsoft*: <https://blogs.microsoft.com/on-the-issues/2017/05/14/need-urgent-collective-action-keep-people-safe-online-lessons-last-weeks-cyberattack/#sm.00000xl4qcz818edarjiw7w28w6qj>

Smith, R. (2018. július 23.): „Russian Hackers Reach U. S. Utility Control Rooms, Homeland Security Officials Say”, letöltve innen, 2018. július 27-én: *Wall Street Journal*: <https://www.wsj.com/articles/russian-hackers-reach-u-s-utility-control-rooms-homeland-security-officials-say-1532388110?emailToken=f9a3eb74337e39394377173dacbbc68e4V/69O5n6wC3K9wgMxw4IuAL+6Ce1fUko-tu3Dlz/SlO9kdm+AcrTba4sqleBWxpGRBmAu2c8M-DZAC4Jf5enBPLZm2wdU>

Snowden, E. (2018. március 17): „@Snowden”, letöltve innen, 2018. augusztus 27-én: *Twitter@Snowden*: <https://twitter.com/snowden/status/975147858096742405?lang=de>

Snyder, T. (dátum nélkül): „Timothy Snyder”, letöltve innen, 2018. szeptember 10-én: *Goodreads*: <https://www.goodre->

ads.com/quotes/8068974-believe-in-truth-to-abandonfacts-is-to-abandon-freedom Snyder, T. (2017): *Über Tyrannei*. München: C.H. Beck.

Sokolov, D. A. (2018. december 20.): „Irreführung beim Datenschutz: Washington verklagt Facebook”, letöltve innen, 2018. december 22-én: *Heise*: <https://www.heise.de/newsticker/meldung/Irrefuehrung-beim-Datenschutz-Washington-verklagt-Facebook-4257054.html>

Sottek, T. C. (2016. szeptember 26.): „Transcript: Here are words Trump just used to talk about ‘the cyber’”, letöltve innen, 2018. július 23-án: *The Verge*: <https://www.theverge.com/2016/9/26/13068578/transcript-here-are-words-trump-just-used-to-talk-about-the-cyber>

Specia, M. (2018. május 16.): „E.U. Official Takes Donald Trump to Task: ‘With Friends Like That’ ...”, letöltve innen, 2018. július 11-én: *The New York Times*: <https://www.nytimes.com/2018/05/16/world/europe/europe-donald-tusk-tweet-trump.html>

Stangl, W. (2011): „Massenpanik – Massenhysterie”, letöltve innen, 2018. augusztus 15-én: I: <http://psychologie-news.stangl.eu/1247/massenpanik-massenhysterie>

Stanton, C. (2019. január 28.): „How Should Countries Tackle Deepfakes?”, letöltve innen, 2019. február 8-án: *Carnegie Endowment For International Peace*: https://carnegieendowment.org/2019/01/28/how-should-countries-tackle-deepfakes-pub78221?utm_source=ctw&utm_medium=email&utm_content=buttonlink&mkt_tok=eyJpIjoiTlRZM01USX-

lOakExTlRndyIsInQiOiJNY1hhXC9wMlcyWE5QRlM-
wa3EzS1MwSG5UNUVLVERrV2loNXN2QzIzWnI2NzVwaTh

Starks, T. (2017. július 21.): „Top White House official talks Cyber Command, international engagement, more”, letöltve innen, 2018. július 22-én: *Politico*: <https://www.politico.com/tipsheets/morning-cybersecurity/2017/07/21/top-white-house-official-talks-cyber-command-international-engagement-more-221454>

Steiner, E. (2018. július 9.): „Enttäuscht von Europa wendet sich Russland nach China”, letöltve innen, 2019. március 5-én: *Welt*: <https://www.welt.de/wirtschaft/article179007162/Wegen-EU-Sanktionen-Russland-wirbt-um-Investitionen-aus-China.html>

Stewart, P. (2018. június 5.): „Deep in the Pentagon, a secret AI program to find hidden nuclear missiles”, letöltve innen, 2018. október 17-én: *Reuters*: <https://www.reuters.com/article/us-usa-pentagon-missiles-ai-insight/deep-in-the-pentagon-a-secret-aiprogram-to-find-hidden-nuclear-missiles-idUSKCN1J114J>

Stocker, F. (2019. január 16.): „Der Dollar verspielt seinen Status als ‘sicherer Hafen’”, letöltve innen, 2019. február 7-én: *Welt*: <https://www.welt.de/finanzen/article187130552/US-Dollar-Warum-die-Waehrung-kein-sicherer-Hafen-mehr-ist.html>

Stockholmi Nemzetközi Békekutató Intézet, SIPRI (2018): *SIPRI Yearbook 2018*. Letöltve innen, 2019. márc. 4-én: *SIPRI*: <https://www.sipri.org/yearbook/2018>

Swan, J. (2019. január 16.): „Trump’s strategic planning inspiration: Mike Tyson”, letöltve innen, 2019. január 16-án: *Axios*: <https://www.axios.com/donald-trump-miketyson-planning-strategy-bc799c7f-d1f2-432e-96e9-9e87d08a01ef.html>

Swan, J., & McCammond, A. (2019. február 3.): „Why Trump swears off planning”, letöltve innen, 2019. február 7-én: *Axios*: <https://www.axios.com/donald-trumpwhite-house-meeting-preparation-eee8f937-a45d-499d-b322-ac-de6b50268c.html>

Tanriverdi, H. (2018. október 5.): „Wie moderne Gesellschaften in den Cyberkrieg abdriften”, letöltve innen, 2018. november 24-én: *Süddeutsche Zeitung*: <https://www.sueddeutsche.de/digital/buch-rezension-zu-cyberwar-wie-moderne-gesellschaften-in-den-cyberkrieg-abdriften-1.4155704>

Szerzőkollektíva Kdo H II 1 (2) (2017): „Thesenpapier II. Digitalisierung von Landoperationen”, szerk. K. Heer, K. D. MGO, & G. F. Leidenberger, letöltve 2019. május 16-án a *Deutsches Heerről*: https://www.deutschesheer.de/portal/a/heer/start/aktuell/nachrichten/jahr2018/marzerz2018/!ut/p/z1/hVBLT4NAEP41XJmF0lq8bdOIVUt-MUQp7MVMYFwzuku1CjPHHu6RJL7VxDpPMfI95gIACHM-KxlWhbrbBzdSkWb4s42iRhxrZJ-MoZz3cvj_k2DZIsGbz2_1-GEg9mV4AaymqB0HjdXPcIIMhAgavIrrchO2ZKyc

Tett, G. (2016. július 1): „Why we no longer trust the experts”, letöltve innen, 2018. augusztus 28-án: *The Irish Times*: <https://www.irishtimes.com/opinion/gillian-tett-why-weno-longer-trust-the-experts-1.2706715>

- The Economist (2018. november 29.): „Russia has emerged as an agricultural powerhouse”, letöltve innen, 2019. január 5-én: *The Economist*: <https://www.economist.com/business/2018/12/01/russia-has-emerged-as-an-agricultural-powerhouse>
- The New York Times (2018. február 16.): „Read the Special Counsel’s Indictment Against the Internet Research Agency and Others”, letöltve innen, 2018. július 24-én: *The New York Times*: <https://www.nytimes.com/interactive/2018/02/16/us/politics/document-The-Special-Counsel-s-Indictment-of-the-Internet.html>
- Theuretsbacher, W. (2014. június 12): „Flugsicherung: Protokoll zweier Störangriffe”, letöltve innen, 2018. november 10-én: *Kurier*: <https://kurier.at/chronik/oesterreich/flugsicherung-protokoll-zweier-stoerangriffe/70.083.561>
- Thomas, T. L. (2004): „Russia’s Reflexive Control Theory and the Military”, in: *Journal of Slavic Military Studies*, 17, 237–256. doi:10.1080/13518040490450529
- Trenin, D. (2017. augusztus 22.): „Looking out Five Years: Ideological, Geopolitical, and Economic Drivers of Russian Foreign Policy”, letöltve innen, 2019. február 14-én: *Carnegie Moscow Center*: <https://carnegie.ru/commentary/72812>
- Trump, D. (1987. szeptember 2.): „An open letter from Donald J. Trump”, letöltve innen, 2018. augusztus 20.: *Factba.se*: <https://factba.se/transcript/donald-trump-letter-foreign-policy-september-2-1987>

- Trump, D. (2015. október 7.): „Speech: Donald Trump in Waterloo, IA”, letöltve innen, 2018. december 26-án: *Factba.se*: <https://factba.se/transcript/donald-trump-speech-waterloo-ia-october-7-2015>
- Trump, D. (2016. március 31.): „Interview: Donald Trump with Woodward”, letöltve innen, 2018. október 5-én innen: *Factba.se*: <https://factba.se/transcript/donald-trump-washingtonpost-transcript-march-31-2016>
- Trump, D. (2016. november. 06.): „Speech: Donald Trump in Minneapolis, MN”, letöltve innen, 2018. augusztus 20-án: *Factba.se*: <https://factba.se/transcript/donald-trump-speech-minneapolis-mn-november-6-2016>
- Trump, D. (2018. december 19.): „#realdonaldtrump”, letöltve innen, 2018. december 21-én: *Twitter*: <https://twitter.com/realdonaldtrump/status/1075721703421042688>
- Trump, D. (2018. július 14.): „Interview: Jeff Glor Interviews Donald Trump in Scotland (Complete)”, letöltve innen, 2018. augusztus 20-án: *Factba.se*: <https://factba.se/transcript/donald-trump-jeff-glor-cbs-news-full-interview-july-14-2018>
- Trump, D. (2018. július 31.): „Speech: Donald Trump Holds a Make America Great Again Rally in Tampa”, letöltve innen, 2018. augusztus 20-án: *Factba.se*: <https://factba.se/transcript/donald-trump-speech-maga-tampa-july-31-2018>
- Trump, D. (2018. augusztus 2.): „Speech: Donald Trump Holds a Political Rally in Wilkes-Barre, PA”, letöltve innen, 2018. augusztus 20-án: *Factba.se*: <https://factba.se/transcript/donald-trump-speech-maga-wilkes-barre-pa-august-2-2018>

Tucker, P. (2014. október 29.): „Major Cyber Attack Will Cause Significant Loss of Life By 2025, Experts Predict”, letöltve innen, 2018. november 27-én: *Defense One*: <https://www.defenseone.com/threats/2014/10/cyber-attack-will-cause-significant-loss-life-2025-experts-predict/97688/>

Tucker, P. (2015. április 20.): „NSA Chief: Rules of War Apply to Cyberwar, Too”, letöltve innen, 2018. május 28-án: *Defense One*: <http://www.defenseone.com/technology/2015/04/nsa-chief-rules-war-apply-cyberwar-too/110572/>

Tucker, P. (2017. október 26.): „How NATO Is Preparing to Fight Tomorrow’s Information Wars”, letöltve innen, 2018. július 28-án: *Defense One*: <https://www.defenseone.com/technology/2017/10/how-nato-preparing-fight-tomorrows-information-wars/142084/?oref=d1-related-article>

Tucker, P. (2019. február 19.): „You Have 19 Minutes to React If the Russians Hack Your Network”, letöltve innen, 2019. február 24-én: *Defense One*: https://www.defenseone.com/technology/2019/02/russian-hackers-work-several-times-faster-chinese-counterparts-new-data-shows/154952/?oref=defenseone_today_nl

United Nations Conference on Trade And Development (2018): *Review of Maritime Transport*. Genf: United Nations.

United States District Court (2017): *MalwareTechBlog Indictment*. Wisconsin: Eastern District of Wisconsin.

United States District Court (2018): *Indictment*. Columbia: Courts for the District of Columbia, letöltve innen, 2018. július 24-

én: <https://d3i6fh83elv35t.cloudfront.net/static/2018/07/Muellerindictment.pdf>

United States District Court (2018. február): *Indictment*. Columbia: Courts for the District of Columbia.

University of Cambridge; DROG (dátum nélkül): „Bad News”, letöltve innen, 2019. február 8-án: *Get Bad News*: <https://get-badnews.com/#intro>

van Creveld, M. (2017): *More on War*. Oxford: Oxford University Press.

Vestner, T. (2018. március 24.). Interjú Tobias Vestnerrel (készítette Y. Hofstetter).

von Clausewitz, C. (1832–34): *Vom Kriege* (II. köt., második könyv: Über die Theorie des Krieges. 3. Kapitel), szerk. W. Hahlwe, Bonn: Dümmler; letöltve innen, 2018. május 28-án: <https://www.clausewitz.com/readings/VomKriege1832/Book2.htm>

Vosoughi, S., Roy, D. & Aral, S. (2018. március 13.): „The spread of true and false news online”, in: *Science*, 359 (6380), 1146–1151. doi:10.1126/science.aap9559

Weigel, G. (2003): *Zeuge der Hoffnung*, Paderborn: Ferdinand Schöningh.

Welt (2018. augusztus 25.): „Dürfen Roboter über Menschenleben entscheiden?”, letöltve innen, 2018. november 1-jén: *Welt*: <https://www.welt.de/politik/ausland/article181301462/Autonome-Waffen-Duerfen-Roboter-ueber-Menschenleben-entscheiden.html>

Westphalen, F. (1971. április): *Der Richter als Revolutionär*.
Köln: Rheinischer Merkur.

Wike, R., Stokes, B., Poushter, J., Silver, L., Fetterolf, J. & Devlin, K. (2018. október 1.): „Trump’s International Ratings Remain Low, Especially Among Key Allies”, letöltve innen, 2018. október 4-én: *Pew Research Center*: <http://www.pewglobal.org/2018/10/01/trumps-international-ratings-remain-low-especially-among-key-allies/>

Wirtschaft.com (2018. június 20.): „Maaßen: Russland für Hekkerangriff auf Stromnetze verantwortlich”, letöltve innen, 2018. július 27-én: *Wirtschaft.com*: <https://wirtschaft.com/maassen-russland-fuer-hekkerangriff-auf-stromnetze-verantwortlich/>

Woodward, B. (2018): *Fear*. New York, N.Y.: Simon and Schuster.
ZDF heute (2017. január 11.): „Trump beschimpft Reporter”, letöltve innen, 2017. január 27-én: *ZDF*: <http://www.heute.de/nach-der-pressekonferenz-donald-trump-und-die-medien-berichterstattung-aus-dem-weissen-haus-46304588.html>

Zeit online (2017. október 30.): „US-Wahlkampf: Facebook zeigte 126 Millionen Nutzern russische Propaganda”, letöltve innen, 2018. szeptember 26-án: *Zeit online*: <https://www.zeit.de/politik/ausland/2017-10/us-wahlkampf-facebook-russland-polit-werbung-einflussnahme>

Zeit online (2018. március 18.): „Ermittlungen gegen Wahlkampfshelfer von Donald Trump”, letöltve innen, 2018. szeptember 24-én: *Zeit online*: <https://www.zeit.de/digital/da->

tenschutz/2018-03/cambridge-analytica-ermittlungen-da-
tenschutzverletzungen-us-wahlkampf

Zuboff, S. (2018): *Das Zeitalter des Überwachungskapitalismus*,
Frankfurt/New York: Campus.

Tartalom

[ELŐSZÓ] A béke kellős közepén

[EGY] A kód mint fegyver

Biztonsági rések

Két út a hatalomhoz

Elkötelezettség a béke iránt

Az állam és a hatalom

A világrend aszimmetriája

Nélkülünk: a helyettesítő keresése

A környezeti intelligencia mint csatatér

Hibrid hadijátékok

Választási titkok

Bizonyítékok hiányában

Adattolvajok

Kritikus infrastruktúrák veszélyben

Hibrid támadások célkeresztjében

[KETTŐ] Információs háború

Semmi sem olyan, mint volt: az új normális

Amikor a kapitalizmus demokráciának látszik

Aki bizalmatlanságot vet, változást arat

Hazugsággal a sikerhez

Politikacsináló narratívák
A médiajelenlét költségei
Cenzúra az interneten
Inger–reakció-játék
Twitterharcosok
A gumiszobában
A véleménytömeg megszervezése
A félelem hulláma
Csak a magamfajtákban bízom
Valóság és mese határán
A felvilágosodás vége
Vigyázat, nyelv! Provokáció és extrémizmus

[HÁROM] Fegyverkezési verseny a mesterséges intelligencia területén

Háború harcosok nélkül?
A drónok támadása
A támadás előtt: érzékelés
Állítsuk meg a gyilkos robotokat!
Automatikus vagy autonóm?
Összhangban a nemzetközi humanitárius joggal?
Szigorúan titkos: az elektronikus harc
Az Achilles-sarok: az elektromágneses spektrum
Elektronikus ellenintézkedések
Hálózatbiztonság mesterséges intelligencia révén

[NÉGY] Visszahekkelés

Joghézagok: a nemzetközi jog tökéletlensége

Ius ad bellum: az erőszak tilalma

A robbanás erejével

Az agresszor keresése

[ÖT] Harc a dominanciáért

Amerika és a profit logikája

Kína rendszeralternatívája: a járadék logikája

A putyinizáció: Make Russia great again

A kínai álom

Szingularitás a csatatéren

A járadék mint technológiai királycsináló

[HAT] „Csak feltételesen védekezésre kész”

Frontvonalban

Utazás cél nélkül

Bátorság a határozott demokráciapolitikához

A hegemoniális hatalom előfeltételei

Európa békéjét és biztonságát szolgáló technológia

Nagyobb biztonság teremtése a környezeti intelligencia számára

A védelem kiépítése

„Nem félnek tőlünk”: elrettentés és eszkaláció

Tűrőképesség teremtése osztott infrastruktúrákkal

A társadalom beoltása a támadások ellen

A vonzerő alapja: az innováció

[ZÁRSZÓ] Amikor az igény találkozik a valósággal

Köszönetnyilvánítás

Jegyzetek

Bibliográfia



www.corvinakiado.hu

Felelős kiadó: Kúnos László, a Corvina igazgatója

Felelős szerkesztő: Blaschtik Éva

Műszaki vezető: Székelyhidi Zsolt

Forgalmazza:

eKönyv Magyarország Kft.



Elektronikus könyv: Ambrose Montanus

Felhasznált betűtípusok

Josefin Sans - SIL Open Font License

Kelly Slab - SIL Open Font License

Noto Serif – Apache License 2.0